Parere sugli schemi di “Linee guida in materia di whistleblowing sui canali interni di segnalazione” e di delibera di modifica e integrazione della Delibera ANAC recante le recante le “Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell’Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali" - 9 ottobre 2025

VEDI ANCHE NEWSLETTER DEL 27 NOVEMBRE 2025

[doc. web n. 10184673]

Parere sugli schemi di “Linee guida in materia di whistleblowing sui canali interni di segnalazione” e di delibera di modifica e integrazione della Delibera ANAC recante le recante le “Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell’Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne" - 9 ottobre 2025

Registro dei provvedimenti
n. 581 del 9 ottobre 2025

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il cons. Angelo Fanizza, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati – di seguito, Regolamento);

VISTO il d.lgs. 30 giugno 2003, n. 196, recante “Codice in materia di protezione dei dati personali” (di seguito, Codice);

VISTA 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 (c.d. “whistleblowing”) (di seguito, Direttiva);

VISTO il parere del Garante sullo schema di decreto legislativo recante attuazione della Direttiva, adottato con provvedimento dell’11 gennaio 2023, n. 1 (doc. web n. 9844945);

VISTO il d.lgs. 10 marzo 2023, n. 24 (Attuazione 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 e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali - di seguito, Decreto), con il quale la Direttiva è stata recepita nell'ordinamento interno;

CONSIDERATO che il Decreto assicura nell'ordinamento interno la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato (art. 1, comma 1, del Decreto);

CONSIDERATO, altresì, che le condotte o le omissioni oggetto di segnalazione possono consistere, in particolare, in violazioni del diritto nazionale (illeciti civili, illeciti amministrativi, illeciti penali, illeciti contabili, condotte illecite rilevanti ai sensi del d.lgs. n. 231/2001, violazioni dei modelli di organizzazione e gestione previsti nel d.lgs. n. 231/2001), nonché in violazioni della normativa dell'Unione europea indicata nell'Allegato 1 al Decreto e di tutte le disposizioni nazionali che ne danno attuazione e che, in tale ambito, sono indicate anche le disposizioni a "tutela della vita privata e dei dati personali e sicurezza delle reti e dei sistemi informativi" (art. 2, comma 1, lett. a), nn. 1-6, e lett. J) All. 1 del Decreto, con specifico riferimento al Regolamento e al Codice);

CONSIDERATO che la persona segnalante è, in base a tale disciplina di settore, la persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo (art. 2, co. 1, lett. g), del Decreto), ovvero nel contesto delle attività lavorative o professionali, presenti o passate, nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all'autorità giudiziaria o contabile (art. 2, comma 1, lett. i), del Decreto);

CONSIDERATO che la tutela approntata dal Decreto si applica non solo se la segnalazione, la denuncia o la divulgazione pubblica avvenga in costanza del rapporto di lavoro o di altro tipo di rapporto giuridico, ma anche anteriormente o successivamente alla costituzione del rapporto giuridico e, in particolare, se le informazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali, o durante il periodo di prova, nonché successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite nel corso dello stesso (art. 3, comma 4, del Decreto);

VISTO quanto disposto dal Decreto, con particolare riguardo a:

- l'ambito di applicazione soggettivo (art. 3);

- i soggetti del settore pubblico e privato obbligati ad attivare canali di segnalazione interna, i quali devono garantire, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione, dovendo i modelli di organizzazione e di gestione, di cui all'art. 6, co. 1, lett. a), del d.lgs. n. 231/2001, espressamente prevedere tali canali di segnalazione interna (art. 4, co. 1);

- la possibilità di affidare la gestione del canale di segnalazione a una persona o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione dello stesso, oppure a un soggetto esterno, anch'esso autonomo e con personale specificamente formato (art. 4, co. 2);

- la possibilità di effettuare le segnalazioni in forma scritta, anche con modalità informatiche, oppure in forma orale, attraverso linee telefoniche o sistemi di messaggistica vocale, oppure, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole (art. 4, co. 3);

la possibilità per i comuni diversi dai capoluoghi di provincia di condividere il canale di segnalazione interna e la relativa gestione, nonché per i soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, non superiore a duecentoquarantanove, di condividere il canale di segnalazione interna e la relativa gestione (art. 4, co. 4);

l'obbligo per i soggetti del settore pubblico, tenuti a nominare il responsabile della prevenzione della corruzione e della trasparenza, di cui all'art. 1, co. 7, della l. 6 novembre 2012, n. 190, di affidare a quest'ultimo, anche nelle ipotesi di condivisione di cui all'art. 4, co. 4, del Decreto, la gestione del canale di segnalazione interna (art. 4, co. 5);

la necessità che la segnalazione interna presentata ad un soggetto diverso da quello previsto dal Decreto sia trasmessa, entro sette giorni dal suo ricevimento, al soggetto competente, dando contestuale notizia della trasmissione alla persona segnalante (art. 4, co. 6);

le modalità di gestione del canale di segnalazione interna (art. 5);

le condizioni per l'effettuazione di una segnalazione esterna all'Autorità Nazionale Anticorruzione (di seguito, ANAC) (art. 6);

i canali di segnalazione esterna presso ANAC, da attivarsi anche tramite il ricorso a strumenti di crittografia, per garantire la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione (art. 7);

le attività che devono essere svolte da ANAC a fronte del ricevimento di una segnalazione esterna e quelle che devono essere svolte dalle competenti autorità amministrative nei casi in cui ANAC abbia provveduto a inoltrare alle stesse una segnalazione esterna avente ad oggetto informazioni sulle violazioni che non rientrano nella propria competenza (art. 8);

le garanzie a tutela dell'identità del segnalante e della riservatezza degli interessati, anche con riguardo alla necessità che i dati siano trattati da personale espressamente autorizzato ai sensi degli artt. 29 e 32, par. 4, del Regolamento e dell'art. 2-quaterdecies del Codice, nonché che la segnalazione sia sottratta all'accesso previsto dagli artt. 22 e ss. della l. 7 agosto 1990, n. 241, e dagli artt. 5 e ss. del d.lgs. 14 marzo 2013, n. 33 (art. 12);

le condizioni al ricorrere delle quali la persona segnalante che effettua una divulgazione pubblica beneficia della specifica protezione prevista dalla legge (art. 15);

le condizioni al ricorre delle quali le persone fisiche possono beneficiare delle misure di protezione previste dalla legge (art. 16);

il divieto di atti ritorsivi nei confronti del segnalante e degli altri soggetti cui la legge ha esteso tale garanzia (quali, in particolare, facilitatori, persone legate al segnalante da stabile rapporto affettivo o di parentela, colleghi di lavoro) (art. 17) nonché gli specifici compiti istituzionali attribuiti ad ANAC al riguardo (art. 19);

la limitazione della responsabilità del segnalante (art. 20) e l'invalidità di rinunce e transazioni che hanno per oggetto i diritti riconosciuti dal Decreto (art. 22);

il regime sanzionatorio derivante dalla violazione delle disposizioni del Decreto (art. 21);

le norme transitorie e l'abrogazione delle disposizioni di cui all' articolo 54-bis del d.lgs. 30 marzo 2001 n. 65, l'art. 6, commi 2-ter e 2-quater, del d.lgs. 8 giugno 2001, n. 231 e l'art. 3

della l. 30 novembre 2017, n. 179 (art. 23 e 24);

CONSIDERATO che il Decreto contiene specifiche disposizioni volte ad assicurare il coordinamento con la disciplina di protezione dei dati, nella prospettiva di tutelare, nel contesto lavorativo e professionale, le persone a vario titolo coinvolte nel processo di presentazione e gestione delle segnalazioni, prevedendo, in particolare, specifiche garanzie, quali: la cancellazione dei dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione; la limitazione dei diritti di cui agli articoli da 15 a 22 del Regolamento, nei limiti di quanto previsto dall' articolo 2-undecies del Codice; il ruolo di titolari del trattamento dei soggetti pubblici e privati in relazione ai trattamenti connessi al ricevimento e alla gestione delle segnalazioni e la necessità di assicurare il rispetto dei princìpi generali in materia di protezione dei dati, nonché di adottare misure appropriate a tutela dei diritti e delle libertà degli interessati, fornendo, altresì, l'informativa sul trattamento dei dati personali agli stessi; la possibilità per taluni titolari del trattamento pubblici e privati di condividere le risorse per il ricevimento e la gestione delle segnalazioni, a condizione di determinare in maniera trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali, agendo in qualità di contitolari del trattamento; la necessità che i titolari del trattamento pubblici e privati definiscano il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione di impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che, in qualità di responsabili del trattamento, trattano dati personali per loro conto (art. 13); il periodo di conservazione della documentazione inerente alle segnalazioni interne ed esterne per il tempo necessario alla gestione delle stesse e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nonché le modalità di documentazione delle segnalazioni presentante oralmente al telefono o nel corso di un incontro con il personale autorizzato (art. 14);

VISTO l'art. 10, comma 1, del Decreto, ai sensi del quale "ANAC, sentito il Garante per la protezione dei dati personali, adotta, entro tre mesi dalla data di entrata in vigore del presente decreto, le linee guida relative alle procedure per la presentazione e la gestione delle segnalazioni esterne. Le linee guida prevedono l'utilizzo di modalità anche informatiche e promuovono il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità della persona segnalante, della persona coinvolta o menzionata nella segnalazione, nonché del contenuto delle segnalazioni e della relativa documentazione";

VISTO il "Parere sullo Schema di Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali – procedure per la presentazione e gestione delle segnalazioni esterne", reso dal Garante, ai sensi del richiamato art. 10, co. 1, del Decreto, con provv. 6 luglio 2023, n. 304, doc. web n. 9912239;

VISTA la Delibera di ANAC n. 311 del 12 luglio 2023 (pubblicata nella Gazzetta Ufficiale Serie Generale n. 172 del 25 luglio 2023), recante le "Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne" (di seguito, le "Linee guida sul canale esterno"), che tengono conto del predetto parere reso dal Garante e anticipano alcuni punti di attenzione anche in relazione ai canali interni di segnalazione;

VISTA la nota del 21 agosto 2025 (prot. del Garante n. 0120460), come integrata con nota del 17 settembre 2025 (prot. del Garante n. 0121654), con la quale ANAC, a seguito di preliminari interlocuzioni con l'Ufficio del Garante, ha trasmesso all'Autorità:

uno schema di delibera di ANAC di approvazione delle “Linee guida in materia di whistleblowing sui canali interni di segnalazione” (di seguito, le “Linee guida sui canali interni”), redatto anche sulla base dei contributi pervenuti nel quadro di una consultazione pubblica; e

uno schema di delibera di ANAC di modifica e integrazione della richiamata Delibera n. 311 del 12 luglio 2023, recente le Linee guida sul canale esterno, predisposta allo scopo di “assicurare la coerenza” con lo schema di Linee guida sui canali interni, nonché di “superare alcune criticità segnalate dai soggetti tenuti ad applicare il d.lgs. 24/2023”;

CONSIDERATO che, stante quanto previsto dal richiamato art. 10, comma 1, del Decreto, ANAC ha chiesto al Garante di rendere il proprio parere sulla versione aggiornata delle Linee guida sul canale esterno, limitatamente alle parti delle stesse oggetto di modifica o integrazione per effetto del predetto schema di delibera, nonché sullo schema di Linee guida sui canali interni, stante la stretta interconnessione tra i due documenti e i rilevanti profili in essi contenuti, che rilevano ai fini della disciplina in materia di protezione dei dati;

RILEVATO che lo schema di Linee guida sui canali interni si articola in una premessa, cinque sezioni (suddivise in diversi paragrafi) e tre partizioni, denominate “Approfondimenti”, e ha ad oggetto, in particolare, con specifico riguardo ai profili rilevanti per la tutela degli interessati nel contesto di trattamento in questione:

la ricostruzione del quadro normativo in materia, le principali novità intervenute per effetto della Direttiva e del Decreto nonché l’oggetto e le finalità delle Linee guida, che sono state predisposte da ANAC “anche tenuto conto del disposto di cui all’art. 8, co. 1, lett. a) del […] decreto [, …] al fine di garantire un’applicazione uniforme ed efficace della normativa sul whistleblowing e indirizzare i soggetti tenuti a dare attuazione alla stessa” (premessa);

l’obbligo per gli enti pubblici e privati, cui si applica la normativa in materia di whistleblowing, di attivare al proprio interno appositi canali per ricevere e gestire le segnalazioni, dovendo gli stessi, tra l’altro, definire, in un apposito atto organizzativo/MOG 231, i compiti e i poteri del soggetto destinatario delle segnalazioni, le modalità per il loro ricevimento e il processo di gestione delle stesse (sez. 2);

le modalità di effettuazione della segnalazione (in forma scritta o orale), privilegiando l’impiego di piattaforme informatiche, tenuto conto che, attraverso strumenti software, è possibile adottare stringenti misure di sicurezza e assicurare un maggiore livello di protezione dei dati personali tanto nella fase di acquisizione delle segnalazioni quanto in quella di gestione delle stesse, nonché, ove le piattaforme siano adeguatamente progettate e configurate, di assicurare la cifratura dei dati a riposo e di mantenere un’interlocuzione riservata con la persona segnalante; ciò fermo restando che lo strumento o servizio informatico impiegato deve essere affidabile, dovendosi valutare, anche in sede di svolgimento della valutazione di impatto sulla protezione dei dati di cui all’art. 35 del Regolamento, l’idoneità delle misure di sicurezza adottate, assicurando, anche nei casi in cui si faccia ricorso a un fornitore esterno, un livello di sicurezza adeguato al rischio, nonché adottando scelte conformi ai principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita di cui all’art. 25 del Regolamento (sez. 2, par. 2.2);

il gestore del canale interno e la sua attività (sez. 3, parr. 3.1-3.3), essendo presi in considerazione anche i casi in cui la fornitura dell’infrastruttura (piattaforma informatica) sia affidata a un fornitore, che tratta i dati quale responsabile del trattamento ai sensi dell’art. 28 del Regolamento (sez. 3, par. 3.4.1); in casi in cui la complessiva gestione del canale di segnalazione sia affidata a un fornitore, che tratta i dati quale responsabile del trattamento ai sensi dell’art. 28 del Regolamento (sez. 3, par. 3.4.2); i casi in cui è consentita una

condivisione del canale di segnalazione tra più soggetti, considerati quali contitolari del trattamento ai sensi dell'art. 26 del Regolamento (sez. 3, par. 3.4.3);

la conservazione della documentazione inerente alla segnalazione e i termini di cancellazione della segnalazione e della relativa documentazione (sez. 3, par. 3.5, punto 5);

i codici di comportamento (sez. 4);

la formazione (sez. 5);

la disciplina whistleblowing e il modello organizzativo 231 (Approfondimento 1);

i gruppi societari (Apprendimento 2);

il ruolo degli Enti del Terzo settore (Approfondimento 3);

CONSIDERATO che l'acquisizione e gestione delle segnalazioni dà luogo a trattamenti di dati personali, anche appartenenti a particolari categorie o relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti a essa allegati, riferiti a interessati (persone fisiche identificate o identificabili) e, in particolare, ai segnalanti o alle persone indicate come possibili responsabili delle condotte illecite o a quelle a vario titolo coinvolte nelle vicende segnalate (cfr. art. 4, par. 1, nn. 1) e 2), del Regolamento);

RITENUTO che i trattamenti di dati personali posti in essere dai soggetti pubblici e privati obbligati a istituire canali di segnalazioni interni - non diversamente da quelli posti in essere da ANAC nell'ambito della gestione del canale esterno di segnalazione e nei procedimenti amministrativi connessi alle competenze attribuitele dal Decreto, nonché da quelli che, in tale ambito, sono posti in essere delle autorità amministrative competenti alla luce dell'oggetto della segnalazione esterna - sono necessari per dare attuazione agli obblighi di legge e ai compiti d'interesse pubblico previsti dalla disciplina di settore, la cui osservanza è condizione di liceità del trattamento (artt. 6, par. 1, lett. c) ed e) e parr. 2 e 3, 9, par. 2, lett. b) e g), 10 e 88 del Regolamento, nonché 2-ter e 2-sexies del Codice);

RITENUTO, in ogni caso, che i predetti soggetti pubblici e privati sono tenuti a rispettare, in qualità di titolari del trattamento, non solo le richiamate diposizioni di settore che costituiscono la base giuridica dei relativi trattamenti, ma anche i principi in materia di protezione dei dati (art. 5 del Regolamento) e che tali soggetti, nell'ambito della necessaria individuazione delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi per gli interessati nel delicato contesto in esame, devono definire il proprio modello di gestione delle segnalazioni in conformità al principio di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (artt. 5, par. 1, e par. 2 , 24, 25 e 32 del Regolamento), tenuto conto anche delle osservazioni presentate al riguardo dal responsabile della protezione dei dati (RPD), ove presente;

CONSIDERATO che lo schema di Linee guida sui canali interni sottoposto all'Autorità tiene conto delle indicazioni fornite, per i profili di competenza, nel corso dell'attività istruttoria e delle interlocuzioni informali intercorse, anche in occasione di specifiche riunioni, tra l'Ufficio del Garante e i rappresentanti di ANAC, al fine di assicurare, nel pieno rispetto della normativa in materia di protezione dei dati personali, la specifica tutela della riservatezza dell'identità del segnalante e della segnalazione - allo scopo di prevenire misure discriminatorie e ritorsive nei confronti del segnalante e degli altri soggetti indicati dalla legge - , garantendo, in pari tempo, il necessario bilanciamento tra l'esigenza di riservatezza della segnalazione, la necessità di accertamento degli illeciti e il diritto di difesa e di contraddittorio del segnalato, considerati, altresì, i rischi sussistenti per tutti gli interessati nel delicato contesto lavorativo e professionale (cfr., audizione del Garante per la protezione dei dati personali sul ddl di delegazione europea 2021-

Senato della Repubblica – 14° Commissione parlamentare dell'Unione europea, 8 marzo 2022, doc. web n. 9751458);

CONSIDERATO che lo schema di Linee guida sui canali interni recepisce il contenuto delle interlocuzioni informali intercorse, con riferimento, in particolare, tra gli altri profili, alla necessità che:

siano gli enti soggetti alle previsioni del Decreto a svolgere, in qualità di titolari del trattamento, la valutazione di impatto sulla protezione dei dati, ai sensi dell'art. 35 del Regolamento, potendo gli stessi eventualmente avvalersi del supporto del fornitore della soluzione tecnologica, anche acquisendo la documentazione a tal fine messa a disposizione dallo stesso (sez. 2, par. 2.2);

nel caso in cui difettino i requisiti per poter considerare una segnalazione rilevante ai fini della normativa in materia di whistleblowing, sia comunque assicurata la riservatezza del segnalante, in ragione della ragionevole aspettativa di riservatezza e tutela della persona che abbia erroneamente assunto di poter beneficiare delle garanzie approntate da detta normativa (sez. 3, par. 3.5, punto 2);

una volta concluse le attività di gestione della segnalazione, il gestore provveda a cancellare sia la segnalazione sia la relativa documentazione al più tardi decorsi cinque anni dalla comunicazione alla persona segnalante dell'esito finale della procedura di segnalazione (v. art. 14, comma 1, del Decreto), fermo restando che potranno essere conservati, nei termini di legge, gli atti e i documenti che afferiscono ai procedimenti avviati e alle iniziative assunte dal datore di lavoro (ad esempio, procedimento disciplinare; trasmissione degli atti alle autorità competenti; ecc.) che abbiano avuto origine in tutto o in parte dalla segnalazione; ciò in considerazione della circostanza che, fatto salvo quanto previsto dall'art. 12, co. 5, del Decreto, tali atti e documenti non dovrebbero, di regola, contenere riferimenti puntuali alla persona segnalante (sez. 3, par. 3.5, punto 5);

i soggetti addetti o coinvolti nel processo di gestione delle segnalazioni ricevano una specifica formazione anche in materia di protezione dei dati personali (sez. 5);

nel caso in cui, all'interno di gruppi societari, una società del gruppo affidi la gestione del canale alla capogruppo, quest'ultima debba essere considerata responsabile del trattamento ai sensi degli artt. 2, comma 1, n. 8, e 28 del Regolamento (Approfondimento n. 2);

gli Enti del Terzo settore - a cui il legislatore ha affidato il compito di fornire alle persone segnalanti misure di sostegno, consistenti in informazioni, assistenza e consulenze a titolo gratuito sulle modalità di segnalazione e sulla protezione dalle ritorsioni offerta dalle disposizioni normative nazionali e da quelle dell'Unione europea, sui diritti della persona coinvolta, nonché sulle modalità e condizioni di accesso al patrocinio a spese dello Stato - prestino i propri servizi nei limiti previsti dalla disciplina nazione ed eurounitaria (art. 18 del Decreto e art. 20 della Direttiva) (Approfondimento n. 3);

RILEVATO CHE le Linee guida sui canali interni, in coerenza con la disciplina in materia di protezione dei dati, chiariscono che, allorquando una società appartenente a un gruppo societario affidi la gestione del canale alla capogruppo, quest'ultima debba essere considerata responsabile del trattamento ai sensi degli artt. 4, comma 1, n. 8, e 28 del Regolamento (v. Approfondimento n. 2 - sezione "L'affidamento della gestione del canale di segnalazione a terzi (o esternalizzazione)"), si ritiene che il documento debba essere conseguentemente aggiornato al fine di superare le ambiguità ancora presenti nel testo (v., in particolare, Approfondimento n. 2, sezione "La condivisione", pag. 34, ove si legge che "si precisa che tutte le società del gruppo, in quanto contitolari del trattamento definiscono, ai sensi dell'art. 26 del Regolamento UE 2016/679, nel

contratto di cui sopra, le responsabilità in merito all'adempimento degli obblighi in materia di privacy);

CONSIDERATO che le intercorse interlocuzioni hanno riguardato anche la necessità di assicurare il pieno coordinamento tra lo schema di Linee guida sui canali interni e le Linee guida sul canale esterno, alla luce delle indicazioni già formalizzate in occasione del citato parere del Garante del 6 luglio 2023, n. 304, con particolare riguardo alla necessità di:

- invitare i segnalanti a utilizzare esclusivamente i canali appositamente istituiti per presentare segnalazioni, considerato che tali canali offrono maggiori garanzie in termini di sicurezza e riservatezza, chiarendo che, anche nell'eventualità in cui una segnalazione sia inviata per errore mediante canali alternativi, debba comunque essere assicurata la riservatezza dell'identità del segnalante e la protezione dei dati di tutti gli interessati (v. sez. 2, par. 2.2);

- precisare che, quando si utilizzino canali e tecniche tradizionali, occorre comunque garantire la riservatezza richiesta dalla normativa di settore, assicurando la protocollazione riservata, ad esempio mediante il meccanismo delle due buste chiuse (v. sez. 2, par. 2.2);

- rammentare che, qualora enti di dimensioni minori condividano il canale di segnalazione interna e la relativa gestione, come previsto dall'art. 4, comma 4, del Decreto, gli stessi, in qualità di contitolari del trattamento, sono tenuti a stipulare un accordo interno ai sensi dell'art. 26 del Regolamento, ferma restando la necessità di adottare misure tecniche e organizzative per garantire che ciascun ente abbia accesso solo alle segnalazioni di propria competenza (sez. 3, par. 3.4.3);

RITENUTO, altresì, che lo schema di Linee guida sui canali interni tiene conto - in coerenza con gli orientamenti dell'Autorità sui trattamenti in ambito lavorativo e nello specifico contesto in esame - di ulteriori profili particolarmente delicati, oggetto di specifiche interlocuzioni e afferenti anche alla sicurezza del trattamento, prevedendo, in particolare, con riguardo all'acquisizione e gestione delle segnalazioni in forma scritta, che:

- il ricorso alla posta elettronica (ordinaria o certificata) sia considerato di per sé non adeguato a garantire la riservatezza dell'identità della persona segnalante, se non accompagnato da specifiche contromisure opportunamente giustificate, quali misure di mitigazione del rischio individuate in sede di definizione della valutazione di impatto sulla protezione dei dati; ciò in quanto, di regola, i sistemi informatici di gestione della posta elettronica generano, raccolgono e conservano, in modo preventivo e generalizzato, i log relativi all'invio e alla ricezione dei messaggi, sussistendo così il rischio che si possa risalire, anche indirettamente, all'identità della persona segnalante, specialmente nel caso in cui quest'ultima utilizzi la casella di posta elettronica fornita dal datore di lavoro (sez. 2, par. 2.2, ove si richiama, altresì, il "Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati", adottato dal Garante il 6 giugno 2024, doc. web n. 10026277);

- nel caso in cui l'accesso ai canali interni di segnalazione avvenga dalla rete dati interna del soggetto obbligato/datore di lavoro, sia garantita la non tracciabilità della persona segnalante nel momento in cui viene stabilita la connessione a tali canali, sia sulle piattaforme informatiche che negli apparati (es. firewall o proxy) eventualmente coinvolti nella trasmissione delle comunicazioni della persona segnalante (sez. 2, par. 2.2);

RILEVATO che il richiamato schema di delibera che modifica e integra la precedente Delibera di ANAC n. 311 del 12 luglio 2023, nella prospettiva di assicurare la coerenza con le Linee guida sui canali interni e di fornire ulteriori indicazioni, anche sulla base delle interlocuzioni intercorse tra l'Ufficio e ANAC, ai soggetti rientranti nell'ambito di applicazione del Decreto, con particolare

riferimento, per quanto attiene alle parti aventi implicazioni in materia di protezione dei dati personali, prevede che:

anche ove si faccia ricorso alla posta elettronica (ordinaria e certificata) quale canale di segnalazione interna, siano individuate specifiche misure di mitigazione del rischio in sede di svolgimento della valutazione di impatto sulla protezione dei dati (v. le modifiche alla parte dedicata all'"Istituzione dei canali di segnalazione", pag. 37);

nell'ipotesi in cui più enti affidino a uno stesso soggetto esterno la gestione delle segnalazioni, sia garantito che ciascun ente acceda esclusivamente alle segnalazioni di propria spettanza, tenuto anche conto dell'attribuzione della relativa responsabilità, dovendo essere adottate misure tecniche e organizzative per garantire che ciascun ente abbia accesso solo alle segnalazioni di propria competenza, nonché che i canali interni siano progettati in modo da consentire un accesso selettivo alle segnalazioni solo da parte del personale autorizzato e rispettare la tutela della riservatezza e la disciplina in materia di protezione dei dati (v. le modifiche alla parte dedicata a "I soggetti cui va affidata la gestione delle segnalazioni", pag. 38);

qualora enti di minori dimensioni condividano il canale di segnalazione interna e le risorse per lo svolgimento delle indagini, ciascuna amministrazione/ente debba nominare comunque un proprio gestore della segnalazione e siano adottate misure tecniche e organizzative per garantire che ciascun gestore abbia accesso solo alle segnalazioni relative al proprio ente, anche tenuto conto dell'attribuzione della relativa responsabilità (v. le modifiche al periodo a pag. 41 della Parte I, par. 3.1);

la riservatezza debba essere garantita anche ove la persona segnalante richieda un incontro diretto con chi tratta la segnalazione (v. le modifiche alla tabella "La tutela della riservatezza dei segnalante", pag. 52, e alla tabella "la tutela della riservatezza del soggetto segnalato e altri soggetti", pag. 56);

CONSIDERATO, altresì, che il predetto schema di delibera di modifica e integrazione della Delibera di ANAC n. 311 del 12 luglio 2023, interviene anche sulle procedure di trasmissione di una segnalazione da parte di ANAC (all. 2) o verso ANAC (all. 3), definendo, in particolare, le modalità di accesso e di utilizzo della piattaforma informatica di ANAC da parte di utenti di organizzazioni esterne (autorità compenti o altri enti) e le relative misure di sicurezza, da aggiornarsi periodicamente, anche al fine di mitigare i rischi connessi al furto di identità digitale, prevedendo, ad esempio, in caso di utilizzo di identità SPID o certificati CNS non precedentemente utilizzati, l'invio di un codice OTP all'indirizzo e-mail dell'utente dell'organizzazione esterna, che dovrà essere inserito per completare la procedura di autenticazione informatica;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Pasquale Stanzione;

TUTTO CIÒ PREMESSO, IL GARANTE

ai sensi degli artt. 36, par. 4, e 58, par. 3, lett. b), del Regolamento, esprime parere, nei termini di cui in motivazione, sugli schemi di "Linee guida in materia di whistleblowing sui canali interni di segnalazione" e di delibera di modifica e integrazione della Delibera di ANAC n. 311 del 12 luglio 2023, recante le recante le "Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che

segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne", predisposti da ANAC.

Roma, 9 ottobre 2025

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Fanizza