

## **IL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI**

**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, RGPD);

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

**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 (art. 4);
- 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 articoli 29 e 32, par. 4, del Regolamento e dell'articolo 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 specifiche garanzie in materia di trattamento dei dati personali, applicabili nell'ambito dell'acquisizione e gestione delle segnalazioni e, in particolare, 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 RGPD, 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 principi 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 i 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 d'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 al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione nonché le modalità anche informatiche di ricezione delle segnalazioni, ovvero oralmente anche attraverso una linea telefonica registrata, un sistema di messaggistica vocale registrato o nel corso di un incontro con il personale autorizzato (art. 14);
- le condizioni al ricorrere 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);
- la limitazione della responsabilità del segnalante (art. 20) l'invalidità di rinunce e transazioni che hanno per oggetto i diritti riconosciuti dal Decreto (art. 22);
- 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);

**VISTA** la nota con la quale il Titolare ha trasmesso al RPD la bozza di DPIA e dello schema di atto organizzativo;

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

**RITENUTO** che i trattamenti di dati personali posti in essere dal Titolare, nell'ambito della gestione del canale di segnalazione interno, 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 RGPD, nonché *2-ter* e *2-sexies* del Codice privacy);

**RITENUTO**, in ogni caso, che il Titolare del trattamento è tenuto a rispettare non solo le richiamate disposizioni di settore che come detto costituiscono la base giuridica dei relativi trattamenti, ma anche i principi in materia di protezione dei dati (art. 5 del RGPD) e che tale soggetto, 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 ai principi della "*protezione dei dati fin dalla progettazione*" e della "*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);

**CONSIDERATO** che il Titolare ha attivato, predisponendo una specifica piattaforma informatica, un canale per le segnalazioni interne che garantisce, anche tramite il ricorso a strumenti di crittografia, 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 (ferma restando la possibilità di presentare una segnalazione anche nel corso di incontri in presenza con il personale autorizzato);

**CONSIDERATO**, più nel dettaglio, che l'impianto procedurale attivato dal Titolare tiene conto delle indicazioni fornite dal Garante per la Protezione dei Dati Personali, in particolare, con riguardo a:

- la possibilità che, anche in caso di segnalazioni prive di dati anagrafici del segnalante, quest'ultimo possa essere, in talune circostanze, identificabile da elementi di contesto, con la conseguenza che tali segnalazioni non possono essere considerate anonime in senso tecnico e sprovviste delle garanzie previste dalla legge;
- la 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, sebbene 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;
- la necessità di chiarire che, nell'ambito delle valutazioni funzionali a garantire la scelta del segnalante in merito ai diversi canali di segnalazione (modalità informatiche o canali tradizionali), il ricorso alla posta elettronica ordinaria e certificata non è di per sé adeguato a garantire la riservatezza, e che, quando si utilizzino canali e tecniche tradizionali, occorre indicare gli strumenti previsti per garantire la riservatezza richiesta dalla normativa, assicurando la protocollazione

- riservata, ad esempio mediante il meccanismo delle due buste chiuse;
- la puntuale definizione di casi in cui il segnalato può - nel corso dei procedimenti eventualmente avviati nei suoi confronti a seguito della conclusione dell'attività di verifica e di analisi della segnalazione -, essere informato dell'esistenza di una segnalazione che lo riguarda; ciò in quanto nell'ambito dei procedimenti, anche disciplinari, conseguenti alla segnalazione, la contestazione potrebbe essere "*fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa*" (art. 12, comma 5, del Decreto), non essendo, pertanto, necessario che, fuori dei casi espressamente previsti dalla legge al predetto comma 5 (contestazione fondata in tutto o in parte sulla segnalazione; conoscenza dell'identità indispensabile per la difesa; consenso espresso del segnalante), il segnalato venga a conoscenza della circostanza che l'accertamento ha avuto origine da una segnalazione;
  - la necessità di considerare quali soggetti autorizzati al trattamento soltanto le persone che, in base alle scelte organizzative del titolare del trattamento, siano competenti a ricevere o a dare seguito alle segnalazioni e siano adeguatamente istruiti al riguardo;
  - l'opportunità di chiarire che i titolari del trattamento devono rendere *ex ante* un'informativa sul trattamento dei dati personali ai possibili interessati (segnalanti, segnalati, persone interessate dalla segnalazione, facilitatori, ecc.) mediante la pubblicazione di documenti informativi (ad esempio tramite sito *web* o piattaforma informatica) o per mezzo di informative brevi in occasione dell'utilizzo degli altri canali previsti dal decreto, non dovendo, invece, fornire agli specifici interessati direttamente coinvolti menzionati da una segnalazione informative su base individuale;
  - l'opportunità di chiarire che, considerato che il trattamento dei dati personali mediante i sistemi di acquisizione gestione delle segnalazioni presenta rischi specifici per i diritti e le libertà degli interessati - in ragione anche della particolare delicatezza delle informazioni potenzialmente trattate, della vulnerabilità degli interessati nel contesto lavorativo, nonché dello specifico regime di riservatezza dell'identità del segnalante previsto dalla normativa di settore - e come espressamente previsto dal Decreto (art. 13, co. 6), i titolari del trattamento devono definire "*il proprio modello di ricevimento e gestione delle segnalazioni [...] sulla base di una valutazione d'impatto sulla protezione dei dati*";
  - l'arco temporale durante il quale occorre garantire la riservatezza del segnalante e degli altri interessati, con particolare riguardo alla circostanza che, stante l'obbligo di conservare la segnalazione non oltre cinque anni a decorrere dalla data dell'esito finale della procedura di segnalazione (art. 14, comma 1, del Decreto), la riservatezza dovrà essere sempre garantita durante tale periodo (fatte salve le ipotesi previste dall'art. 12, commi 3-5, del Decreto), e che, decorso tale periodo, dovendo la segnalazione essere cancellata, verrebbe comunque meno la possibilità di risalire all'identità del segnalante;
  - l'opportunità di chiarire che, nell'ottica di privilegiare la volontà del segnalante, è sempre possibile per quest'ultimo ritirare la segnalazione mediante apposita comunicazione da trasmettere attraverso il canale originariamente prescelto per l'inoltro della stessa, specificando le conseguenze derivanti da tale scelta in merito alla prosecuzione o meno degli accertamenti eventualmente già avviati;
  - l'opportunità di chiarire, nel caso in cui sia palese l'assoluta irrilevanza rispetto alla vicenda segnalata di parti della segnalazione, che contengono dati personali, le modalità con le quali è possibile assicurare la cancellazione dei dati prevista dall'art. 13, comma 2, del Decreto;

**RITENUTO**, altresì, che, con riferimento ai profili relativi alla sicurezza del trattamento,

nell'ambito dell'acquisizione e gestione delle segnalazioni tramite piattaforma informatica:

- sono state adottate misure tecniche e organizzative tali da garantire un'adeguata sicurezza del trattamento dei dati personali, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali, fermo restando che tali misure saranno, comunque, periodicamente riesaminate e aggiornate;
- nel contesto in esame, caratterizzato da elevati rischi per i diritti e le libertà degli interessati, il ricorso a strumenti di crittografia nell'ambito del canale interno è da ritenersi una misura adeguata a dare attuazione, fin dalla progettazione e per impostazione predefinita, al principio di integrità e riservatezza, garantendo la tutela dei dati personali trattati nel processo di segnalazione, sia nella fase di trasmissione che di conservazione;
- nel caso in cui l'accesso al canale interno di segnalazione avvenga dalla rete dati interna del soggetto obbligato, è garantita la non tracciabilità del segnalante nel momento in cui viene stabilita la connessione a tale canale, sia sulla piattaforma informatica che negli apparati (es. firewall o proxy) eventualmente coinvolti nella trasmissione delle comunicazioni del segnalante;
- sia effettuato, ove possibile, il tracciamento delle operazioni svolte dal personale autorizzato alla gestione delle segnalazioni, nel rispetto delle garanzie a tutela del segnalante e degli altri soggetti menzionati, al fine di consentire la verifica della liceità e correttezza del trattamento e garantire la sicurezza del trattamento (parte prima, par. 4.1.3), nel rispetto delle garanzie previste dalla disciplina di settore in materia di controlli a distanza (art. 4 della l. n. 300/1970, nonché art. 114 del Codice; v. anche art. 88 del Regolamento);

**RITENUTO** di non dover formulare osservazioni sulla bozza di Atto organizzativo, atteso che le indicazioni fornite in precedenza dal sottoscritto RPD sono state tenute in debita considerazione;

**VISTA** la documentazione in atti;

### **TUTTO CIÒ PREMESSO, IL RPD**

ai sensi dell'articolo 39, paragrafo 1, lett. C) del RGPD, esprime parere favorevole sulla valutazione d'impatto sulla protezione dei dati personali, condotta dal Titolare del trattamento, la quale conclude nel senso di ritenere "possibile procedere con l'attivazione dei canali di segnalazione interni e l'avvio del trattamento senza ulteriori misure tecniche e organizzative".