ECOPACK S.p.A.
Via della Masolina 24
10040 Piobesi Torinese (TO)
Email: info@ecopack.com
Telefono: 011 965 7657

Information on the processing of personal data ex art. 13-14 Regulation (EU) 2016/679

Stakeholders: persons who report wrongdoing

ECOPACK S.p.A. as Data Controller of your personal data, pursuant to and for the purposes of EU Regulation 2016/679 hereinafter 'GDPR', hereby informs you that the aforementioned legislation provides for the protection of data subjects with respect to the processing of personal data and that such processing will be based on the principles of correctness, lawfulness, transparency and protection of your confidentiality and your rights.

Your personal data will be processed in accordance with the legal provisions of the aforementioned legislation and the confidentiality obligations therein and in compliance with the provisions of Legislative Decree No. 24 of 10 March 2023 on Whistleblowing.

Legal basis for processing:
Personal data processed in the 'whistleblowing' procedure of the whistleblower and related third parties:

- common data: name, surname, job role, etc., defence pleadings, content of the report (b.g. legal obligation art. 6 par. 1 lett. c - consent of the data subject art. 6 par. 1 lett. a - ascertain, exercise or defend a legal claim Art. 9 par. 2 lett. f GDPR);
- special data (i.e. religious or philosophical beliefs or trade union membership or health-related data (b.g. specific obligations of the Data Controller under employment law Art. 9 par. 2 lett. b - ascertaining, exercising or defending a right in court Art. 9 par. 2 lett. f GDPR)
- personal data relating to criminal convictions and offences (b.g. legal obligation Art. 6 par. 1 lett. c - Art. 10 GDPR)

Purpose of processing: Your personal data and the data of the persons connected with the report will be processed for the following purposes related to the whistleblowing procedure:

- Obligatory legal obligations, in accordance with Law No. 179 of 30 November 2017, as amended (b.g. legal obligation)
- Acquisition and management of reports of unlawful conduct of which it has become aware by reason of its employment, service or supply relationship (b.g. legal obligation)
- Investigative activities aimed at verifying the validity of the reported fact and the adoption of consequent measures (b.g. legal obligation)
- Disclosure of the report, as well as any personal identification data, to competent and authorised third parties or authorities (b.g. consent of the person concerned)
- Disclosure of the identity of the whistleblower for the purpose of defending the accused (b.g. consent of the person concerned)
- Gestione della segnalazione tramite linea telefonica registrata o altro sistema di messagistica vocale, nonché al fine di documentare la segnalazione in un incontro diretto (b.g. consenso del soggetto interessato)
- Defence investigation activities to seek and identify evidence to establish, exercise or defend a right in a court of law (b.g. legitimate interest)

The processing of functional data for the fulfilment of these obligations is necessary for the proper management of the report, and their provision is mandatory for the implementation of the purposes indicated above. The Data Controller also makes it known that any failure to provide, or incorrect communication of, any of the mandatory information may result in the Data Controller being unable to guarantee the appropriateness of the processing itself. The processing of personal data based on Art. 6(1)(a) is not obligatory, its provision is optional, and you therefore have the right to revoke your consent at any time without prejudice to the lawfulness of the processing. Failure to give consent will make it impossible for the Data Controller to follow up the disciplinary procedure on the oral report and to document the report in the face-to-face meeting.

Method of treatment: Your personal data may be processed in the following ways:

- processing by means of electronic computers,
- manual processing by means of paper archives.

All processing is carried out in compliance with the methods set out in Articles 6, 32 of the GDPR and through the adoption of appropriate security measures.

Communication: your data may be communicated, if necessary for the performance of the services requested, to competent and duly appointed parties for the performance of the services necessary for the proper management of the report (by way of example but not limited to: the manager of the report, the company appointed to manage the platform); external consultants involved in the preliminary investigation (e.g. law firms); at the outcome of any preliminary investigation to the competent authorities for the notification of the proceedings (Judicial Authority, Court of Auditors, ANAC) with a guarantee of protection of the rights of the data subject. Your data will be processed only by personnel expressly authorised by the Data Controller.

Diffusion:Your personal data will not be disseminated in any way.

Conservation period: Please note that, in compliance with the principles of lawfulness, purpose limitation and data minimisation, pursuant to Article 5 of the GDPR, the retention period of your personal data for purposes related to the whistleblowing legislation is:

- 60 days from the completion of the relevant checks for reports that have been assessed as non-significant and filed on the basis of the company procedure, after which they will be deleted
- or no later than 5 years from the date of the communication of the final outcome of the alert procedure for all other alerts and their handling documentation

Rights of the Data Subject

Ai sensi degli artt. Da art.15 e seguenti del GDPR, ferme eventuali limitazioni derivanti dalle disposizioni cogenti, ovvero ai sensi dell'art. 2-undecies del d.lgs. 101/2018, si prevede che:

1. The data subject shall have the right to obtain confirmation as to whether or not personal data concerning him/her exist, even if not yet recorded, and communication of such data in intelligible form.
2. The person concerned has the right to be informed about:
   a. the origin of the personal data
   b. the purposes and methods of processing
   c. the logic applied in the event of processing carried out with the aid of electronic instruments
   d. the identity of the data controller, data processors and the representative designated pursuant to Article 5(2)
   e. of the entities or categories of entity to whom or which the personal data may be communicated or who or which may get to know said data in their capacity as designated representative(s) in the State's territory, data processor(s) or person(s) in charge of the processing.

3. The person concerned has the right to obtain:
   a. the updating, rectification or, where interested therein, the integration of the data;;
   b. the cancellation, transformation into anonymous form or blocking of data processed unlawfully, including data whose retention is unnecessary for the purposes for which the data were collected or subsequently processed
   c. certification to the effect that the operations as per letters a) and b) have been notified, as also related to their contents, to the entities to whom or which the data were communicated or disseminated, unless this requirement proves impossible or involves a manifestly disproportionate effort compared with the right that is to be protected;
   d. portability of the data.
4. The person concerned has the right to object, in whole or in part:
   a. for legitimate reasons to the processing of personal data concerning him/her, even if pertinent to the purpose of collection;
5. The data subject has the right to request the restriction of processing.

You can exercise your rights by sending an email to info@ecopack.com or by sending a written request to the addresses specified above.

Furthermore, if the interested party believes that the processing of their data is contrary to the legislation in force, they can lodge a complaint with the Supervisory Authority for the protection of personal data pursuant to art. 77 of Regulation 2016/679 or submit a report pursuant to art. 144 of Legislative Decree 101/2018.

ECOPACK S.p.A.
Via della Masolina, 24
Piobesi Torinese(TO) – CAP 10040
Tel 011 965 7657 - Email: info@ecopack.com
P.I/C.F.05469550015

1. AMBITO DI APPLICAZIONE

[illegible]

2. CANALI DI SEGNALAZIONE

[illegible]

- [illegible]
  - [illegible]
  - [illegible]
- [illegible]
- [illegible]

[illegible]

- when the legal relationship has not yet begun, if the information on the violations was acquired during the selection process or in other pre-contractual phases;
- during the employment relationship;
- after the dissolution of the legal relationship if the information on the violations was acquired during the relationship.

The whistleblowers, thus identified, will be protected by the company through the protection measures applied pursuant to Chapter III of the Legislative Decree. 24/2023 and in compliance with the obligation of confidentiality (art. 12 Legislative Decree 24/2023), the legislation on the processing of personal data (art. 13 Legislative Decree 24/2023), the prohibition of retaliation (art. 17 Legislative Decree 24/2023) and limitations of liability (art. 20 Legislative Decree 24/2023). The protections provided also apply to the following categories of subjects, as they are potentially exposed to retaliation following the report:

- - facilitators, natural person who assists the reporter in the reporting process, operating within the same working context;
- - people from the same working context as the reporting person and who are linked to him or her by a stable emotional or kinship bond within the fourth degree;
- - entities owned by the reporting person or for which he works;
- - entities that operate in the same working context as the reporting person (e.g. colleagues in the same operational area);
- - work colleagues of the reporting person, who work in the same working context as the reporting person and who have a usual and current relationship with said person;

- entities owned exclusively or in majority ownership by third parties.

3. SUBJECT OF THE REPORT

The report may concern information, including well-founded suspicions, regarding violations committed or which, based on concrete elements, could be committed within the scope of the company's activity.
By violations we mean behaviours, acts or omissions which damage the public interest or the integrity of the Administration and which consist of administrative, accounting, civil or criminal offenses as well as offenses committed in certain sectors falling within the scope of application of the European Union or national acts.
Also included are those violations which have not yet been committed, but which are believed to be capable of being committed based on concrete elements, such as irregularities and anomalies which the reporting party believes could give rise to a violation.

As an example:

- *failure to respect the timing of administrative procedures*
- *accounting irregularities*
- *corruption and fraud*
- *money laundry*
- *violation of environmental and workplace safety regulations*
- *violation of the legislation on the protection of personal data (Privacy) and IT security.*

The following complaints cannot be reported:

- *claims or requests linked to a personal interest of the reporting party, which relate exclusively to their individual work or public employment relationships, or inherent to their work or public employment relationships with hierarchically superior figures*
- *notizie palesemente prive di fondamento, le informazioni che sono già totalmente di dominio pubblico, nonché le informazioni acquisite solo sulla base di indiscrezioni o vociferazioni scarsamente attendibili.*
- *violations for which specific reporting procedures are already provided for governed by European Union or national legislation referred to in art. 1, paragraph 2 letter. b), of the Decree, as well as reports relating to certain sectors for which the application of the reference provisions referred to in the art. 1, paragraph 2 letter. c), and paragraphs 3 and 4 of the Decree*

We remind you to take care to clearly and completely report all the elements useful for carrying out the checks and investigations necessary to evaluate the validity of the report, namely:

- describe precisely the illicit conduct which is the subject of the report
- indicate the personal details of the person and/or office held responsible for the illicit conduct

- describe the circumstances of time and place of the illicit conduct
- attach all available documents to support the report

4. REPORTING REQUIREMENTS

The reports:

- **must be made in good faith**
- must be detailed and based on **precise factual elements**
- they must concern facts that can be **verified and known directly by the person reporting**
- must contain **all the information necessary to identify the perpetrators** of the illicit conduct.

It is recommended to use the internal reporting channel responsibly, avoiding making unfounded or bad faith communications, as such actions could lead to legal or disciplinary consequences.

5. REPORTING MANAGEMENT

The company has provided, in compliance with the legislation, an internal IT reporting channel provided by a third party, which operates as data controller pursuant to art. 28 of Regulation (EU) 2016/679 (hereinafter GDPR), equipped with encryption tools, designed to guarantee the confidentiality of the identity of the reporter, of the person involved and of the person mentioned in the report, as well as of the content of the reporting and related documentation.
The management of reports is entrusted to a competent authorized external party appointed as responsible pursuant to art. 28 GDPR, with related legal support in the event of preliminary investigations.
The procedure guarantees that the management of reports is entrusted to subjects who are not in situations of conflict of interest.

ECOPACK S.p.A.
Via della Masolina, 24
Piobesi Torinese(TO) – CAP 10040
Tel 011 965 7657 - Email: info@ecopack.com
P.I/C.F.05469550015

6. METHOD OF REPORT SUBMITTING

The report - via the internal IT channel - can be reached via the link https://ecopack.sibilus.io/ also present on the institutional website for potential external reporting parties.

The Reporter, during the reporting procedure, must follow the following recommendations, contained in the IT platform:

- *Do not use a company PC and/or a device connected to the company network/intranet;*
- *Provide as much data and information as possible;*
- *The anonymous report will be taken into consideration only if adequately detailed and with all the information useful to verify it regardless of knowledge of the identity of the reporter;*
- *The company reserves the right not to follow up on unsubstantiated anonymous reports, which will be considered inadmissible and therefore archived;*
- *Regularly check, via the "Find report" section of the platform, the status of the report and communicate with the company, also answering any questions;*
- *Indicate whether a natural person who works in the same work context assisted you in making the report (Facilitator)*
- *Do not enter personal data that could lead to your identity in the description of the reported fact;*

The IT platform guarantees, as per the regulations, the different reporting methods to the reporter:

- by completing the form and sending a written report;

- via the form, a report is sent in oral form, through a recorded voice messaging system present within the same IT channel. In this case, the report, subject to the consent of the reporting person, is documented by the manager using a device suitable for storing and listening to the audio file or by full transcription; in the latter case, the reporting person can verify, rectify or confirm the content of the transcript by signing it.

- via form by organizing a direct meeting, set within a reasonable time, with the manager of the report. In this case, the report, subject to the consent of the reporting person, is documented by the manager by recording on a device suitable for storage and listening or by means of a report. The reporting person can verify, correct and confirm the minutes of the meeting by signing them. The report thus acquired must be inserted into the dedicated IT platform, which will report the investigation process as well as the follow-up to the report itself.

La segnalazione deve contenere obbligatoriamente le seguenti informazioni:

- circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione;
- descrizione del fatto;
- Generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati.

Il sistema informatico provvede alla cifratura e alla memorizzazione della segnalazione, separandola dall'identità del segnalante e inviando la notifica di arrivo al gestore della segnalazione e la notifica di avvenuta ricezione al segnalante entro 7 giorni.

Il segnalante potrà seguire l'iter della segnalazione mediante la sezione "**Trova segnalazione**" inserendo il codice OTP rilasciato dalla piattaforma contestualmente all'invio della segnalazione, avendo la possibilità di integrare la segnalazione e di rispondere, mediante il sistema di messaggistica (chat e/o note) del medesimocanale informatico, ad eventuali richieste del gestore delle segnalazioni.

Ogni segnalazione ricevuta da un soggetto diverso dal gestore delle segnalazioni autorizzato, per cui al di fuori del suddetto canale, dovrà essere veicolata entro 7 giorni dalla ricezione al soggetto competente, tramite la sezione "**Inoltra segnalazione**" nella piattaforma.

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento dellasegnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza nonché del principio di cui agli articoli 5, paragrafo 1, lettera e), del GDPR e, ove applicabile, 3, comma 1, lettera e), del decreto legislativon. 51 del 2018.

7. ISTRUTTORIA DELLE SEGNALAZIONI

Qualora, in fase di istruttoria, ovvero in fase di valutazione preliminare si riscontri l'insussistenza delle condizioni essenziali previste per la segnalazione e per le relative tutele accordate al segnalante, la stessa sarà ritenuta inammissibile dandone motivata comunicazione al segnalante.

In particolare, la segnalazione è considerata inammissibile ed è direttamente archiviata nelle seguenti ipotesi:

a) manifesta infondatezza per l'assenza di elementi di fatto riconducibili alle violazioni tipizzate di cui nell'art. 2, comma 1 lett. a), del Decreto e richiamate nell'art. 3 delle presenti Linee guida;
b) manifesta insussistenza dei requisiti soggettivi previsti dalla normativa per l'effettuazione della segnalazione;
c) manifesta incompetenza della società sulle questioni segnalate;
d) accertato contenuto generico della segnalazione di illecito tale da non consentire la comprensione dei fatti, ovvero segnalazione di illeciti corredata da documentazione non appropriata o inconferente tale da non far comprendere il contenuto stesso della segnalazione;
e) produzione di sola documentazione in assenza della segnalazione di condotte illecite;
f) mancanza dei dati che costituiscono elementi essenziali della segnalazione, indicati all'art. 5 della presente procedura.

Nei casi di cui alle lettere d) ed f), ove la segnalazione non sia adeguatamente circostanziata, il gestore delle segnalazioni può chiedere al segnalante eventuali elementi integrativi, mediante il canale informatico dedicato ovvero anche di persona ove il segnalante abbia richiesto un incontro diretto.

Valutata l'ammissibilità della segnalazione, il gestore della segnalazione avvia l'istruttoria sui fatti o sulle condotte segnalate per verificare la sussistenza degli stessi. Il gestore delle segnalazioni mantiene le interlocuzioni con la persona segnalante, chiedendo alla medesima le integrazioni necessarie per le finalità istruttorie.

Nel corso della disamina istruttoria la persona coinvolta – e cioè la persona menzionata nella segnalazione come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata – può essere sentita ovvero, su sua richiesta, è sentita, anche mediante l'acquisizione di osservazioni scritte e documenti. Restano fermi gli obblighi di riservatezza in particolare nell'ambito di fattispecie di possibile rilevanza penale.

All'esito dell'istruttoria - e fuori dai casi di archiviazione per le ragioni di inammissibilità - il gestore delle segnalazioni dà seguito alla segnalazione adottando le misure necessarie.

Qualora la segnalazione abbia da oggetto illeciti che rilevano sotto il profilo penale o erariale, il gestore delle segnalazioni archivia la medesima e ne dispone l'immediata trasmissione alla competente Autorità giudiziaria o contabile, evidenziandone il carattere di segnalazione di cui al Decreto e dunque l'adozione delle cautele atte a garantire il rispetto delle disposizioni normative in materia, restando disponibile a fornire all'Autorità giudiziaria, ove richiesto, il nominativo del segnalante o eventuali ulteriori elementi istruttori.

Nel caso in cui si provveda all'inoltro della segnalazione all'Autorità competente, dandone comunicazione al segnalante, eventuali successive integrazioni dovranno essere direttamente trasmesse dal segnalante medesimo all'Autorità giudiziaria.

Qualora la segnalazione abbia ad oggetto illeciti di rilievo disciplinare, il gestore delle segnalazioni ne dispone l'archiviazione e la trasmissione all'ufficio competente.

Il gestore delle segnalazioni provvede a fornire riscontro alla segnalazione, dandone comunicazione al segnalante entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione.

Il riscontro è finalizzato a comunicare al segnalante le informazioni relative al seguito dato alla segnalazione e cioè l'azione intrapresa per valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate o da adottare.

ECOPACK S.p.A.
Via della Masolina, 24
Piobesi Torinese(TO) – CAP 10040
Tel 011 965 7657 - Email: info@ecopack.com
P.I/C.F.05469550015

8. OBBLIGO DI RISERVATEZZA

L'identità della persona segnalante e qualsiasi altra informazione da cui questa possa evincersi, anche indirettamente, non sono rivelate, senza il consenso espresso del segnalante medesimo, a persone diverse da quelle incaricate per la gestione delle segnalazioni espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del GDPR e dell'articolo 2-quaterdecies del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

Nell'ambito del procedimento penale e del procedimento innanzi alla Corte dei conti l'obbligo di riservatezza è garantita nei modi e nei limiti previsti dall'articolo 12, commi 3 e 4, del Decreto.

Nell'ambito del procedimento disciplinare, l'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità. In tal caso il gestore delle segnalazioni provvede ad avvisare previamente la persona segnalante mediante comunicazione scritta delle ragioni per le quali si ritiene necessaria la rivelazione dei dati riservati.

Medesimo avviso alla persona segnalante è dato altresì, nella procedura di segnalazione interna, quando la rivelazione della sua identità nonché le informazioni dalle quali può evincersi, anche indirettamente, tale identità sia indispensabile, anche ai fini della difesa della persona coinvolta, previo consenso espresso del segnalante stesso.

La richiesta di svelamento dell'identità avverrà tramite piattaforma attraverso la sezione "**Richiedi Svelamento identità**" con opportuna motivazione. Il soggetto segnalante tramite l'accesso alla propria area di gestione della propria segnalazione potrà fornire o meno il consenso allo svelamento dell'identità.

In caso di mancato consenso, il gestore della segnalazione sarà obbligato ad archiviare il caso o a valutare di inoltrare la segnalazione alle autorità o uffici competenti.

La tutela dell'identità delle persone coinvolte e delle persone menzionate nella segnalazione è assicurata fino alla conclusione dei procedimenti avviati in ragione della segnalazione e nel rispetto delle medesime garanzie previste in favore del segnalante. La tutela della riservatezza è altresì assicurata in favore del facilitatore, e cioè la persona fisica che assiste il segnalante nel processo di segnalazione, operante nel medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata.

La segnalazione e la documentazione ad essa allegata sono sottratte all'accesso documentale di cui agli articoli 22 e seguenti della legge 7 agosto 1990, n. 241 nonché all'accesso civico generalizzato previsto dagli articoli 5 e seguenti del decreto legislativo 14 marzo 2013, n. 33.

9. TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali, compresa la comunicazione alle Autorità competenti, è effettuato dalla società, in qualità di Titolare del trattamento dei dati personali, a norma del GDPR e del Codice e, ove applicabile, del decreto legislativo 18 maggio 2018, n. 51. I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

Agli interessati viene fornita dalla società apposita informativa, accessibile direttamente nella sezione "**FAQ-Sezione Documenti**" della piattaforma oppure in una sezione dedicata sul proprio sito internet, in merito al trattamento dei dati personali, ai sensi dell'art. 13 del GDPR. Gli stessi possono esercitare in qualsiasi momento i diritti di cui agli articoli da 15 a 22 del GDPR nei limiti di quanto previsto dall'art. 2-undecies del D.lgs. 101/2018.

La società garantisce un livello di sicurezza adeguato ai rischi specifici derivanti dai trattamenti effettuati, sullabase di una valutazione d'impatto sulla protezione dei dati, e disciplinando il rapporto con i fornitori esterni che trattano dati personali per loro conto, ai sensi dell'articolo 28 del GDPR.

10. CANALE DI SEGNALAZIONE ESTERNA

Ferma restando l'attivazione in via prioritaria del canale interno alla società, la persona segnalante ha la possibilità di effettuare una segnalazione attraverso un canale esterno, attivato e gestito dall'ANAC. Il ricorso al canale esterno è consentito qualora ricorra una delle seguenti condizioni espressamente previste:

a) il segnalante ha già effettuato una segnalazione interna ai sensi delle disposizioni precedenti, ma la stessa non ha avuto seguito;

b) il segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;

c) il segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

La procedura per la segnalazione attraverso il canale esterno è disciplinata dalle Linee guida emanate dalla competente Autorità (ANAC).

Le segnalazioni esterne possono essere effettuate in forma scritta o in forma orale o mediante un incontro diretto, secondo le modalità fissate con le medesime Linee guida ANAC.

Il gestore della segnalazione provvede a trasmettere all'ANAC, mediante la procedura prevista dalla stessa Autorità, entro sette giorni dalla ricezione, eventuali segnalazioni esterne erroneamente pervenute alla società, dando contestuale notizia della trasmissione alla persona segnalante.

11. DIVULGAZIONE PUBBLICA

Il soggetto segnalante ha la possibilità di effettuare una divulgazione pubblica sulle condotte illecite commesse dall'azienda, beneficiando delle protezioni previste dal Decreto, qualora:

- non è stato dato riscontro nei termini previsti in merito alle misure previste o adottate per dare seguito alla segnalazione

- il soggetto segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse
- il soggetto segnalante ha fondato motivo di ritenere che la segnalazione esterna possa comportare un rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze.

12. DENUNCIA ALL'AUTORITA' GIUDIZIARIA O CONTABILE

Il soggetto segnalante può denunciare alle Autorità competenti le violazioni commesse o che potrebbero essere commesse dall'azienda, in applicazione delle garanzie previste dal Decreto.

13. DISPOSIZIONE FINALE

Per tutto quanto non espressamente previsto nelle presenti Linee guida si applicano le disposizioni contenute nel Decreto nonché nelle Linee guida ANAC.