

WHISTLEBLOWING

Information on the processing of personal data pursuant to Articles 13 and 14 of Reg. (EU) 2016/679 ('GDPR')

Introduction

Hereinafter, LCI - Lavorazione Carta Riciclata Italiana SRL as Data Controller, provides information on the processing of personal data of data subjects carried out in the framework of the management of whistleblowing reports, i.e. of unlawful conduct or breaches as referred to in Article 2.1(a) of Legislative Decree no. 24/2023 (hereinafter referred to as the '**Whistleblowing Decree**'), including those of the organisation, management and control model pursuant to Legislative Decree 231/2001 as amended [*in the case of MOG*]

According to GDPR, 'data subjects' are the natural persons to whom the data relate. In this case, the persons concerned are the reporting person, the reported person and any persons named in the report.

Reports may be made through the channels and modalities provided for in the whistleblowing procedure (hereinafter, '**Procedure**') and in particular:

- a) in writing, through the appropriate software platform available at the link <https://lci.segnalazioni.info/#/>;
- b) orally, using the specific functionality available through the aforementioned software platform, with the acquisition of the corresponding audio file;
- c) in exceptional cases, at the request of the whistleblower, in an in-person meeting (to be requested in any case via the online platform).

1. Data Controller

The Data Controller is LCI SRL, Tax Code and VAT number 04139540266, with registered office in Viale della Repubblica 193/B 31100 (TV), tel. 0422 693111, e-mail address privacy@lci-srl.it (hereinafter, '**Controller**').

2. Data Protection Officer/Privacy Officer

The Data Protection Officer (hereinafter, '**DPO**') can be contacted at privacy@lci-srl.it

3. Categories and source of processed data

The following data will be processed as part of the whistleblowing report:

- Personal and contact data of the whistleblower, if voluntarily disclosed by him/her;
- Data on the reported person and other persons involved in the report, potentially including data on the committing of unlawful acts;
- Data on the work activity carried out within the company organisation;
- Any other data (potentially also particular data, if relevant to the report) contained in the report or acquired during the investigation phase.

The data of the whistleblower, the reported person and/or third parties are provided directly by the whistleblower himself and/or acquired in the course of the ensuing investigation activities.

4. Purposes of processing, legal bases and data retention periods

Why is personal data processed?	What is the legal basis for the processing?
For the handling of whistleblowing reports, including investigative activities following the report.	The fulfilment of a legal obligation to which the Controller is subject, as provided for in Article 6(1)(c) of GDPR.
If necessary, for the purpose of taking measures following the report and, in general, for the protection of the holder's rights.	Legitimate interest of the Controller under Article 6 1(f) of GDPR.
For the disclosure of the identity of the whistleblower (if known) in the only cases provided for by law, e.g. to enable the whistleblower to defend himself in disciplinary proceedings, (Article 12 par. 5 and 6 of the Whistleblowing Decree).	Consent of the person concerned pursuant to Article 6 1(a) of GDPR

For the documentation of a report made by means of the recorded voice messaging system, by further recording on a device suitable for storage and listening, or by means of a verbatim transcription (Article 14 para. 2 of the Whistleblowing Decree).	Consent of the person concerned pursuant to Article 6 1(a) of GDPR
For the handling of any data, included in the report or revealed during the investigation, relating to criminal convictions and offences or related security measures.	The processing is authorised by the EU or Member State law (specifically, by the Whistleblowing Decree), as provided for in Article 10 of GDPR
For the handling of special data (i.e. data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life) relevant to the reporting case.	Processing is permitted for reasons of substantial public interest (specifically, to comply with the provisions of the Whistleblowing Decree) and/or processing is necessary to ascertain, exercise or defend a right in court, pursuant to Article 9 para. 2 (f) and (g) of GDPR

What is the data retention period?

Data are retained for a maximum period of five years from the date of communication of the final outcome of the procedure for handling the report, unless judicial or disciplinary proceedings are instituted as a consequence of the report itself. In that case, the data will be retained for the entire duration of the proceedings, until their conclusion and the expiry of the time limits for any appeals.

Personal data that are clearly not useful for the handling of a notification alert are not collected or, if accidentally collected, are deleted immediately.

After the above-mentioned retention periods have elapsed, the data will be destroyed, deleted or anonymised, subject to technical deletion and backup times.

5. *Nature of data provision*

At the reporting stage, the provision of data is at the discretion of the whistleblower, it being understood that overly general and unsubstantiated reports cannot be handled effectively.

In the investigation phase, the data controller may acquire further data, either by requesting them from the data subjects or by conducting its own investigations.

The whistleblowing procedure guarantees the confidentiality of the identity of the whistleblower (if disclosed), from the moment of receipt and in any subsequent contact, as well as of the persons who are the subject of the whistleblowing or otherwise mentioned in the whistleblowing.

In any case, anonymous reports will only be taken into account if they are adequately substantiated, based on factual elements and made with full particulars, being such as to make the facts reported appear credible.

6. *Data recipients*

Personal data relating to the handling of the above-mentioned reports are processed by the following entities:

- TMC SRL, as Reporting Manager on behalf of the Data Controller, designated as Data Processor pursuant to Article 28 of Reg. (EU) 2016/679;
- Siatec S.r.l., supplier of the whistleblowing software platform, designated as Data Processor pursuant to Article 28 of Reg. (EU) 2016/679.

Any sharing of the report and documentation produced by the whistleblower with other corporate functions or external professionals for the purpose of investigation is carried out in compliance with the Procedure and the Whistleblowing Decree, with the utmost care to protect the confidentiality of the whistleblower and the reported person, omitting any disclosure of data that is not strictly necessary.

It is understood that the identity of the whistleblower (and any other information from which it can be inferred, directly or indirectly) will not be disclosed, without the whistleblower's consent, to parties other than the Handlers of the reports and (when necessary) to the professionals assisting them in the investigation, without prejudice to the requirements of the applicable legislation.

The data may be disclosed to the Judicial Authority and to other public entities entitled to receive them, such as ANAC, in the cases and in the manner provided for by the Whistleblowing Decree and the Procedure.

In the context of possible criminal proceedings, the identity of the whistleblower is covered by confidentiality in the manner and within the limits provided for in Article 329 of the Code of Criminal Procedure.

In the context of any proceedings before the Court of Auditors, the identity of the whistleblower may not be revealed until the investigation phase is closed.

7. Data transfers outside the EU

Data are not transferred outside the European Union.

8. Features of the software platform for sending reports

The platform for sending reports has the following features:

- It uses the open source software Globaleaks, developed following the OWASP development guidelines and already used by ANAC for the realisation of its OpenWhistleblowing portal;
- is provided and maintained by the supplier Siatec S.r.l., without competition from the Controller's Information Systems;
- only generates anonymous logs in relation to the activities carried out by the whistleblower, in order to prevent his or her identification;
- is protected by security measures appropriate to the risk, including first and foremost the encryption of stored data.

9. Rights of the data subject

It is possible to exercise, in relation to the data processing described above, the rights recognised by the GDPR for data subjects, including the right to:

- request access to the data and information referred to in Article 15 (purpose of processing, categories of personal data, etc.);
- obtain the rectification of inaccurate data or the integration of incomplete data pursuant to Article 16;
- request the deletion of personal data in the cases provided for in Article 17, if the Controller no longer has the right to process them;
- obtain the restriction of processing (i.e. the temporary submission of data to storage only), in the cases provided for in Article 18 GDPR;
- object at any time, for reasons relating to special situations, to the processing of their personal data on the basis of legitimate interest within the meaning of Article 6.1(f) of GDPR.

To exercise your rights, you may contact the DPO by sending an e-mail to privacy@lci-srl.it or, at the data subject's discretion, to the Reporting Managers, via the Platform or at info@siatec.it.

Data subjects have the right to lodge a complaint with the Garante per la Protezione dei Dati Personali (Italian Data Protection Authority) or to take legal action if they consider that the processing of their personal data is contrary to current legislation.

It should be noted that, pursuant to Article 2-undecies of Legislative Decree No. 196/2003 ("Privacy Code"), the rights set out in Articles 15 to 22 of GDPR may not be exercised if the exercise thereof would result in actual and concrete prejudice to the confidentiality of the identity of the whistleblower. In such cases, the rights in question may be exercised through the Personal Data Protection Authority, in the manner set out in Article 160 of the Privacy Code.