

Whistleblowing Data Processing Policy

Reporting irregularities. Internal channel.

Pursuant to Arts. 13 and 14 of Regulation 2016/679/EU (hereinafter "GDPR"), Confezioni e Facon S.r.l., abbreviated as Cieffe S.r.l., with registered office at Via dell'Artigianato, 23 – 26029 Soncino (Cr) (hereinafter referred to as the "Company"), in its capacity as "Data Controller", announces that the personal data of Whistleblowers reporting irregularities in the company's activities will be collected and processed for the management of such irregularities, in compliance with the law, in order to guarantee rights, fundamental freedoms and dignity, particularly with reference to confidentiality and personal identity.

Whistleblowers, to whom this policy is addressed, are all those subjects who, having some relationship with the Data Controller, i.e. the Company, could, in the event of retaliation due to a whistleblowing report submitted, suffer a professional, economic or reputational impact or, in general, an impact detrimental to the person's freedoms and fundamental rights.

In this context, the subjects generally most involved and vulnerable are internal or external collaborators of the Company.

Origin, type of data processed, purpose and legal basis

The processing of the personal data of the Whistleblower and the Party subject to the report, provided directly or collected by authorised or delegated third parties, is carried out by the Company in order to meet obligations deriving from laws, regulations and EU legislation.

The processing is carried out on the following data:

- a) personal and identification data in general;
- b) data relating to the employment relationship between the Whistleblower and/or the Party subject to the report and the Company, such as feedback on the fulfilment of work, legal and responsible conduct obligations with respect to colleagues, customers, suppliers and all parties involved in the Company's activities, i.e., the community and the environment;
- c) data relating to irregularities committed by the Parties subject to the report;
- d) data necessary for the identification of both Whistleblowers and Parties subject to the report;
- e) data relating to third parties involved in the reporting and/or investigation process resulting from the report;
- f) still images, video, audio, movies;
- g) Contact details: emails, mobile phones, messaging apps .

The data may also include those that Art. 9 of the GDPR refers to as "special" data (sensitive data), which reveal the most confidential information about the individual, such as, for example, those relating to health, religious beliefs, inability to work or judicial data concerning criminally relevant conduct of the Subjects.

These data are processed, in compliance with legislation and the Authorisations issued by the Personal Data Protection Authority, for the exclusive purpose of meeting legal obligations, in particular, the legislation defined as "Whistleblowing Management", set forth in Italian Legislative Decree no. 24/2023 for the application of EU Directive 1937/2019.

The processing is carried out to comply with the above-mentioned legislation, aimed at protecting Whistleblowers from any retaliatory actions carried out after they report an irregularity committed within the scope of the company.

The legal bases of the processing for the purposes set forth are: Art. 6.1.c of the Regulation, i.e., the fulfilment of a legal obligation, and Article 6.1.a, i.e. explicit consent in the event that the Whistleblower intends to disclose his or her identity during the procedure. Failure to provide the data or refusal to provide them as completely as possible would make it impossible for the Company to carry out the activities necessary to resolve the irregularities reported.

Communication and dissemination

In compliance with the law, the personal data of the Whistleblower may be disclosed, if the latter has provided consent, to third parties, internal or external to the Company, belonging to the following categories:

- in their own corporate work environment, work colleagues, managers, supervisors, members; the Supervisory Body (if any);
- external data processors pursuant to Article 28 of the GDPR or autonomous data controllers with respect to the Company such as, for example: technological platforms for process management; consultants of various types, engaged to manage reports; lawyers; private investigators; computer forensic technicians; third-party companies;
- Law Enforcement; Judicial Authority; other government entities.

The data will not be disseminated.

All employees, consultants and temporary workers who, authorised to perform processing, carry out their activities on the basis of instructions received from the Company, pursuant to Art. 29 of the GDPR, are appointed as "parties authorised to perform data processing" and receive adequate operating instructions from the Company, particularly with regard to the adoption of and compliance with security measures, in order to guarantee data confidentiality and security. The Employee is invited to report to the Company any circumstances that may result in a potential data breach in order to allow for an immediate assessment and the adoption of measures aimed at countering such an event.

This is without prejudice to the Company's obligation to communicate the data to the competent Authorities at their specific request.

Transfer abroad

The data are processed within the EU and, if necessary, in countries that are deemed adequate with respect to the GDPR.

Processing methods and storage time

The data are processed lawfully and fairly for the purposes set forth above in compliance with the fundamental principles established by legislation.

Personal data may be processed by means of computer or electronic devices or on hard copy, adopting the necessary technical and organisational measures suitable to guarantee security, confidentiality and the reduction of the risks of destruction or loss, even accidental, unauthorised access or unlawful processing.

The data will be processed by the Company for the entire duration of the collaboration relationship and subsequently for the time necessary to resolve the irregularities reported. In any case, the maximum storage period may not exceed 5 years.

Rights of the Whistleblower

The Employee is granted the following rights under the GDPR:

- a) access to personal data and any information relating to their processing;
- b) rectification of inaccurate personal data;
- c) deletion of data;
- d) restriction of processing and objection (when possible);
- e) data portability from the Company to another Data Controller or receipt in a structured, commonly used and machine-readable format;
- f) complaint to the Italian Data Protection Authority .

To obtain more information on the processing of your personal data or to exercise your rights, you can contact Ms Marina Forte (privacy contact point/party responsible for the procedure).

Confezioni and Facon S.r.l., abbreviated as Cieffe S.r.l.

Document generated on 17-12-2023