

PRIVACY POLICY WHISTLEBLOWING

WHISTLEBLOWER

Under Article 13 of Regulation (EU) 2016/679 regarding the processing of personal data concerning the reporting of violations as per Legislative Decree 24/2023

Under Article 13 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter "GDPR") and the applicable legislation concerning the protection of personal data, we inform you that the personal data provided by you, as a Reporting Person (hereinafter also referred to as the 'Data Subject') reporting a violation pursuant to Legislative Decree 24/2023, will be processed in accordance with the aforementioned legislation and in compliance with the principles of fairness, lawfulness, and transparency by personnel authorized by the Company under Article 29 of the GDPR and Article 2-quaterdecies of the personal data protection code (Legislative Decree 196/2003).

Data controller

Data controller is COMPLIFE ITALIA Via Guido Rossa, 1 20024 Garbagnate Milanese (MI) - Italy

Purposes of processing and legal basis

The personal data is processed for the management of internal reports of alleged violations, namely behaviors, acts, or omissions that harm public interest or the integrity of public administration or private entities, as defined by Article 2, paragraph 1, letter a) of Legislative Decree 24/2023, of which the Reporting Person has become aware in the course of their collaboration with the Data Controller. The personal data processed includes those contained in the internal report, and/or in acts and documents attached to it that refer to the Reporting Person and any other potentially involved party.

The personal data may also be processed for conducting necessary investigative activities aimed at verifying the validity of the reported concerns, as well as, if necessary, for adopting adequate corrective measures and initiating appropriate disciplinary and/or legal actions against those responsible for the violations. The legal basis legitimizing the processing of personal data is the fulfillment of a legal obligation to which the Data Controller is subject (Article 6, paragraph 1, letter c) of the GDPR), specifically provided by Legislative Decree 24/2023. The processing may also concern special categories of personal data and data relating to criminal convictions and offenses if included in the report, as provided for by Articles 9 and 10 of the GDPR.

The worker's identity may also be disclosed to other parties.

Categories of data recipients

The personal data provided will be processed by the personnel appointed to manage Whistleblowing reports as authorized individuals by the Data Controller, and by other involved company functions. This is done to follow up on and respond to the received reports, in compliance with the provisions of Legislative Decree



24/2023, and to activate any disciplinary system if necessary. Additionally, corrective actions will be taken to prevent similar situations to those reported.

In the event that the Company entrusts a third party with the management of the reporting channel, the aforementioned personal data will be processed by this third party as a Data Processor appointed by the Data Controller in accordance with Article 28 of the GDPR. These data will be processed exclusively by expressly authorized personnel and in compliance with the provisions of Legislative Decree 24/2023.

The personal data will not be subject to disclosure but may be transmitted to the Judicial Authority. None of the collected data will be transferred to Third Countries, understood as countries not belonging to the European Economic Area (EEA). In case the report is external and is submitted, as provided by articles 6 and 7 of Legislative Decree 24/2023, to the National Anti-Corruption Authority (ANAC), information regarding the processing of personal data will be provided by the Authority itself through appropriate channels.

The criteria for retention periods

Internal reports and related documentation will be retained for the time necessary for handling the report, not exceeding five years from the date of communication of the final outcome of the reporting procedure. This is in compliance with confidentiality obligations as per Article 12 of this Legislative Decree 24/2023, and the principle outlined in Articles 5, paragraph 1, letter e) of the GDPR and 3, paragraph 1, letter e) of Legislative Decree 51 of 2018. After the maximum period of five years, the information related to the report may be retained by the Company to ensure and preserve its right to defense and provide evidence, if required, of the proper management of received reports. In such cases, the personal data of the Reporting Person will be anonymized.

The data processing methods

The processing of personal data will be carried out exclusively by specifically authorized personnel, ensuring the confidentiality of the Reporting Person's identity and the content of internal reports and related documentation. This will be achieved by adopting technical and organizational measures to protect them from unauthorized or unlawful access, destruction, loss, alteration, and disclosure, even accidental. To ensure the confidentiality of the Reporting Person throughout the handling of the internal report, their identity will be known only to individuals expressly authorized to manage such reports. Except in cases where liability for slander and defamation arises under the provisions of the Penal Code or Article 2043 of the Civil Code, or where applicable in criminal proceedings and within the limits established by Article 329 of the Code of Criminal Procedure, the identity of the Reporting Person is protected in all subsequent contexts following the report. Therefore, subject to the aforementioned exceptions, the identity of the Reporting Person cannot be disclosed without their explicit consent, and all individuals who receive or are involved in managing the report are required to protect the confidentiality of this information.



The provision of data

The provision of personal data is optional. However, the lack of providing such data could affect the investigation of the report. Anonymous reports, in fact, will only be considered if adequately detailed and provided with an abundance of particulars, in order to highlight facts and situations related to specific contexts.

Rights of the data subjects

The rights under Articles 15-22 of the GDPR can be exercised within the limits set forth by Article 2-undecies, paragraph 3, of Legislative Decree 196/2003, by contacting the Data Controller or the Data Protection Officer, where designated, using the above-mentioned contact details. Specifically, these identified rights cannot be exercised by directly requesting the Data Controller or the Data Protection Officer, if designated, or by filing a complaint under Article 77 of the GDPR with the Supervisory Authority, if the exercise of these rights could result in actual and concrete prejudice to the confidentiality of the identity of the person reporting violations they became aware of due to their employment relationship or role performed. The exercise of these rights may, in any case, be delayed, limited, or excluded with a reasoned communication provided promptly by the Data Controller, unless such communication could undermine the purpose of the limitation, for the time and within the limits necessary and proportionate, considering the fundamental rights and legitimate interests of the Reporting Person, the involved parties, or those variously involved in the reports. In such cases, according to Article 2-undecies, paragraph 3, of Legislative Decree 196/2003, the Data Subject has the option to exercise these mentioned rights through the Supervisory Authority, as specified in Article 160 of the aforementioned legislative decree. If it is believed that the processing of personal data is in violation of the GDPR, it is possible to lodge a complaint with the Supervisory Authority, as provided by Article 77 of the GDPR (excluding the limitations on the exercise of rights as set out in Article 2-undecies, paragraph 3, of Legislative Decree 196/2003), or to take legal action (Article 79 of the GDPR).

