Whistleblowing and privacy information

CENTRIC

Whistleblowing and privacy information

"WHISTLEBLOWING" PROCEDURE FOR RECEIVING AND MANAGING REPORTS pursuant to Legislative Decree no. 10 March 2023. 24

Summary

Premises

Since its establishment IT Centric S.p.A. (hereinafter, the “Company”) undertakes to create and maintain the necessary conditions so that the relationships established with all its Employees, Collaborators, Consultants, but also Shareholders, Suppliers and Partners always take place in a corporate context of transparency, integrity and responsibility. This is the way IT Centric S.p.A. has always done business. runs his own business. With a view to continuous improvement and in line with the current evolution of the applicable legislation, IT Centric S.p.A. has decided to give a strong signal of respect for the aforementioned principles, strengthening its organizational structures and formalizing a company procedure for receiving and managing internal reports, also through the adoption of a new Procedure for receiving and managing internal reports ("Protocol Whistleblowing"), in compliance with Legislative Decree 10 March 2023 n. 24.

Who can report - Protected subjects

Anyone can use the internal reporting channels to communicate possible violations of the law or alleged illegal conduct of which they have become aware due to their relationship with the Company. The subjects protected by the legislation against any retaliation or discriminatory conduct are employees, former employees, interns, collaborators, consultants, volunteers, trainees, shareholders, people with administrative, management, control, supervision or representation functions at the company, as well as facilitators and colleagues of the whistleblower who have a regular and current relationship with the whistleblower.

How to report

The Company has established internal reporting channels, managed by an independent external company. The channels are:

1) in written form:

- by accessing the web platform https://whistleblowing.noverim.it/itcentric;
- by sending a letter by ordinary mail (simple and/or registered letter) to the Manager's address: Noverim S.r.l. Benefit Society, Piazza degli Affari n. 3, Milan 20123, taking care to indicate on the envelope: **"personal confidential - Whistleblowing report"** and in the text of the letter indicate the name of the company.

2) in oral form, through a direct meeting with the Manager or with one of his delegates specially trained in the matter and appointed for this purpose also pursuant to privacy legislation. The meeting will be guaranteed within 20 working days of the request, to be sent to whistleblowing@noverim.it. The report in oral form, subject to the written consent of the reporting person, is documented by the Manager, by recording on a device suitable for storage and listening or by full transcription. In case of transcription, the Reporter must verify, rectify or confirm the content of the transcription through his signature.

It is necessary that the report is as detailed as possible.

In particular, for the purposes of the eligibility screening, it is necessary that the following essential elements are clear from the report:

- and circumstances of time and place in which the reported event occurred;
- description of the facts being reported with detail on the circumstantial information;
- how the facts covered by the report became known;
- personal details of the person reported or other elements that allow identification.

The identifying data of the reporting person (name, surname, place and date of birth) as well as a contact number (e-mail and telephone number) to which subsequent updates are communicated are optional.

It is advisable, where possible, to also attach documents certifying the validity of the facts being reported, as well as the indication of other subjects potentially aware of the facts.

What to report

The subject of the report can be all behaviors or facts which, in the opinion of the reporter, constitute or are potentially capable of configuring civil, criminal, administrative and accounting offenses and are detrimental to a public or private interest. This channel can be used to report violations, i.e. behaviors, acts or omissions, which damage the integrity of the Company or the public interest, referable - by way of example and not exhaustively - to:

- violations of laws and regulations (national and European);
- acts of corruption;
- corporate fraud;
- human rights;
- behavior that causes damage or prejudice, even if only to its image, to the Company.

The report cannot have as its object:

- disputes, claims or requests linked to a personal interest of the reporting person which relate exclusively to their individual working relationships or inherent to their working relationships with hierarchically superior figures;
- news clearly lacking foundational, information acquired solely on the basis of unreliable indiscretions or rumors (so-called rumours);
- information that is already totally in the public domain.

How reports are managed

Within 7 days of receipt, an acknowledgment of receipt of the report will be given and within 3 months of this notice, feedback will be provided on the follow-up that is given or intended to be given to the report.

In any case, the Reports Manager can interface with the reporter if he deems any further information necessary or start a dialogue aimed at acquiring clarifications or documents.

It is always possible to request a meeting with the person managing the reports through the reporting channels.

Guarantee of confidentiality and protections

Absolute confidentiality is guaranteed to the reporter, the facilitator and the people involved in the report. Any form of personal or professional retaliation for reporting is not permitted or tolerated. If you believe you have suffered retaliation as a result of reporting, you can report it to the National Anti-Corruption Authority (ANAC).

All processing of personal data is carried out in compliance with the legislation on the protection of personal data. See Privacy Policy Attachment.

Please remember that anyone who abuses the protections provided for in this Protocol, reporting manifestly unfounded or opportunistic facts or acts, for the sole purpose of harming the reported person or other subjects, will be held responsible in disciplinary proceedings and in any other competent body.

In the case of ordinary reports made to one's manager and/or hierarchical superior, the protections provided by the Whistleblowing Decree are not guaranteed, unless the Reporter specifies or shows a willingness to benefit from the aforementioned protections.

•••

For further details on the reporting procedure, please refer to the Protocol published on the company intranet or in the Company's management system. In any case, it is always possible to request a copy by sending an e-mail to the following address whistleblowing@noverim.it.

ANNEX A

INFORMATION REGARDING THE PROCESSING OF PERSONAL DATA pursuant to articles 13 and 14 of Regulation (EU) 2016/679 IN RELATION TO REPORTS OF "WHISTLEBLOWING"

IT Centric S.p.A. (hereinafter "Company") informs that personal data (including any sensitive data, such as racial and ethnic origin, religious and philosophical beliefs, political opinions, membership of political parties, trade unions, as well as personal data suitable to reveal the state of health and sexual orientation) of the Reporters, the Reported Party and other subjects possibly involved (collectively, "Personal Data"), acquired during the management of the Reports, will be processed in full compliance with what is established by the regulations in force regarding the protection of personal data and will also be limited to those strictly necessary to verify the validity of the Report and to manage it.

1. Purpose of the processing

The data provided by the Reporting Party for the purpose of representing the alleged illicit conduct of which he has become aware due to his relationship with the Company committed by the subjects who in various capacities interact with the same, are processed for the purpose of carrying out the necessary investigative activities aimed at verifying the validity of the fact being reported and the adoption of the consequent measures.

2. Type of data processed

The reception and management of reports gives rise to processing of so-called personal data. "common" (name, surname, job role, etc.), as well as may give rise, depending on the content of the reports and the deeds and documents attached to them, to the processing of so-called personal data. "particulars" (data relating to health conditions, sexual orientation or trade union membership, referred to in Article 9 GDPR) and personal data relating to criminal convictions and crimes (referred to in Article 10 GDPR).

3. Legal basis of the processing and methods of processing

The legal basis of the processing of Personal Data is identified in the art. 6, paragraph 1, letter. c) of Regulation (EU) 2016/679, i.e. fulfillment of a legal obligation to which the data controller is subject.
With reference only to the conservation of Personal Data following the closure of the reporting management procedure, the legal basis is represented by the legitimate interest of the Data Controller and of the interested parties in the exercise of their rights, in all cases where it is necessary (e.g. opening of disciplinary and judicial proceedings, requests for compensation for damages related to the report).

Pursuant to art. 5 of the GDPR, the data processed as part of the management of reports must be processed in a lawful, correct and transparent manner, collected for specific, explicit and

legitimate purposes, adequate, relevant and limited to those strictly and objectively necessary to verify the validity of the report, accurate and if necessary updated.

During the activities aimed at verifying the validity of the Report, all necessary measures will be adopted to protect the data from accidental or illicit destruction, loss and unauthorized disclosure.

If the report proves to be unfounded, the data must not be kept beyond the deadline established by law for filing a complaint or complaint.

Based on the provisions of the legislation on personal data and Legislative Decree no. 24/2023, the Data Controller, the Data Processor and the persons authorized to process personal data are required to respect the following fundamental principles:

- process the data in a lawful, correct and transparent manner towards the interested parties ("lawfulness, correctness and transparency");
- collect data only for the purpose of managing and following up on reports made by subjects protected by Legislative Decree 24/2023 ("purpose limitation");
- ensure that the data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization'). Personal data that is clearly not useful for processing a specific report will not be collected or, if collected accidentally, will be deleted without delay;
- ensure that the data is accurate and, if necessary, updated; all reasonable steps must be taken to promptly erase or rectify inaccurate data relating to the specific report being handled ('accuracy');
- ensure a ban on tracking of reporting channels;
- guarantee, where possible, the tracking of the activity of authorized personnel in compliance with the guarantees protecting the whistleblower, in order to avoid the improper use of data relating to the report. The tracking of any information that could lead to the identity or activity of the reporter must be avoided.

4. Scope of communication and data transfer

The Personal Data collected in the context of receiving and managing the report will not be disclosed abroad or disclosed in any way.
Exclusively for the purposes indicated, the Personal Data may be communicated to third parties to whom the Company and/or the Manager may entrust certain activities (or part of them); these subjects will operate as independent Data Controllers or will be designated Data Controllers and are essentially included in the following categories:

- Consultants (Law firms, etc.);
- Companies in charge of the administration and management of personnel;
- Investigative agencies;
- Institutions and /o Public Authorities, Judicial Authorities, Police Bodies.

5. Storage of personal data

The Company stores personal data according to the terms set out in the art. 14 of Legislative Decree no. 24/2023, i.e. for the time necessary to process the report and in any case for no more than 5 years from the date of communication of the final outcome of the Report to the Manager. Personal data that is clearly not useful for processing a specific report are not collected or, if collected accidentally, are promptly deleted.

6. Rights of the interested party

The interested party, in the persons of the Reporter or the Facilitator, has the right to access at any time the data concerning him or her and to exercise the rights provided for by articles 15 to 22 of the GDPR, as applicable (right of access to personal data, the right to rectify them, the right to obtain their cancellation or the so-called right to be forgotten, the right to limit processing, the right to portability of personal data or the right to object to processing), by sending an e-mail at the address: whistleblowing@noverim.it. Furthermore, the interested party has the right to lodge a complaint with the Guarantor for the protection of personal data.

7. Data Controller and Persons Authorized to Process

The Data Controller of the Personal Data collected as part of the Internal Reporting is the Company.

The Manager, specifically appointed as Data Processor pursuant to art. 28 GDPR, as well as the Competent Internal Person have been authorized to process personal data by the Company, from which they have also received adequate operating instructions.