NOTICE ON THE PROCESSING OF PERSONAL DATA PURSUANT TO ARTICLES 13 AND 14 OF REGULATION (EU) 2016/679 ("GDPR") ARISING FROM THE SYSTEM ADOPTED BY THE COMPANY FOR COLLECTING REPORTS OF UNLAWFUL CONDUCT OR VIOLATIONS OF THE ORGANIZATION, MANAGEMENT, AND CONTROL MODEL IN ACCORDANCE WITH LEGISLATIVE DECREE 231/2001

	DATA CONTROLLER	**COBO S.p.A.** **Registered Office:** Leno (BS), via Tito Speri, n. 10 – 25024 – Italy **VAT Number:** IT019315300982 **Fiscal Code:** 08976960156 **E-mail:** gdpr@cobogroup.net ("**Company**" o "**Controller**")

TYPES OF DATA PROCESSED AND SOURCE OF DATA

The Company allows detailed reports of illegal conduct of an administrative, accounting, civil, or criminal nature, also pursuant to Legislative Decree 231/2001, or of violations of:

- the Organization, Management, and Control Model adopted by the Company, as well as the related procedures;
- the Code of Ethics;
- acts or omissions that harm the financial interests of the Union;
- acts or omissions concerning the internal market, including violations of European Union competition and State aid rules;
- violations of European Union acts or national acts implementing EU acts, related to specific sectors indicated in the annex to Directive (EU) 2019/1937;

digitally through the "My Whistleblowing" platform ("Platform").

Reports can be nominal or anonymous. In the case of nominal reports, at the whistleblower's discretion, the whistleblower's personal data will be associated with the report. In the case of anonymous reports, the company's IT systems will not be able to identify the whistleblower from the portal access point (IP address).

Within the form provided on the Platform, the whistleblower may indicate their personal data in the case of nominal reports (specifically, personal identification data and contact information), as well as personal data of the reported individual and/or any third parties (hereinafter referred to as the "Data").

The whistleblower's data, if provided, is directly supplied by the whistleblower and thus acquired by the Data Controller from the data subject pursuant to Article 13 of the GDPR; the data of the reported individual and/or third parties is provided by the whistleblower and thus acquired by the Data Controller from third parties pursuant to Article 14 of the GDPR.

Additionally, in the context of this activity, special categories of data (e.g., health-related data) and judicial data (particularly data related to criminal offenses) may also be processed if directly provided by the whistleblower; these categories of data are not mandatorily required for the submission of the report.

PURPOSE OF PROCESSING	LEGAL BASIS FOR PROCESSING	DATA RETENTION PERIOD
Management of detailed reports of unlawful conduct or violations of the Management Model, including investigative activities aimed at verifying the validity of the reported facts and the adoption of consequent measures as provided for in the Management Model.	Compliance with a legal obligation pursuant to Art. 6 of Legislative Decree 231/2001, as amended by Law 179/2017, and Directive (EU) 2019/1937 as implemented by Legislative Decree 24/2023, which requires the Data Controller to provide specific channels for submitting reports in the Management Model, where adopted. Legitimate interest of the Data Controller concerning activities carried out following reports. With specific reference to special categories of data, the legal basis for processing is found in the provisions of Art. 9, para. 2, letter (b) of the GDPR (to fulfil an obligation or exercise a right in the field of labour law).	The Data will be retained for a period of **5 years** from the closure of all activities consequent to the verification of the facts reported, provided that the report does not result in the initiation of a dispute or disciplinary proceedings against the reported individual or the whistleblower. In the latter case, the Data will be retained for the entire duration of the dispute or extrajudicial proceedings until the expiration of the appeal action periods. An exception to the aforementioned five-year retention period applies to reports whose content is entirely unrelated to the purposes of the whistleblowing channel (e.g., complaints, insults, suggestions), which will be deleted within two months from the completion of the analysis, documenting the reasons why they were deemed irrelevant.
If necessary, to establish, exercise, or defend the rights of the Data Controller in judicial proceedings.	Legitimate interest of the data Controller.	
Upon expiration of the above-mentioned retention periods, the Data will be destroyed, deleted, or anonymized, in accordance with the technical procedures for deletion, backup, and accountability of the Data Controller.		

MANDATORY REQUIREMENT FOR DATA PROVISION
The information marked with an asterisk (*****) is mandatory, and failure to provide such information will make it impossible to proceed with the reporting process through the Platform. Provision of the whistleblower's Data is optional. If the Data is not provided, the report will be submitted anonymously.

METHODS OF PROCESSING
The Data will be processed using paper-based, electronic, or automated tools (the "My Whistleblowing" platform) in accordance with the purposes indicated above and in a manner that ensures the security and confidentiality of the Data. Specific security measures are observed to prevent data loss, unlawful or improper use, and unauthorized access.

DATA RECIPIENTS

The Data may be disclosed to entities acting as independent data controllers, such as, by way of example, judicial authorities and other public entities authorized to request them, as well as individuals, companies, associations, or professional firms that provide assistance and consultancy services in this field.

The Data may also be processed, on behalf of the Data Controller, by the service provider managing the Platform, as well as the storage of the information and Data contained therein, to whom appropriate operational instructions are given and who is specifically appointed as the data processor pursuant to Article 28 of the GDPR.

In exceptional cases, if the Company initiates disciplinary proceedings against the reported individual based solely on the report, the whistleblower's Data may be disclosed to the reported individual exclusively to allow the latter to exercise their right of defence.

SUBJECTS AUTHORIZED TO PROCESS DATA

The Data may be processed by members of the supervisory body ("OdV") that receives and manages the report as provided for in the Management Model, as well as by Company personnel who act based on specific instructions regarding the purposes and methods of processing. Such personnel will only be involved in strictly necessary cases, ensuring the absolute confidentiality of the data subjects.

TRANSFER OF DATA TO NON-EU COUNTRIES

No data transfers outside the European Economic Area (EEA) are envisaged for the processing activities in question.

RIGHTS OF THE DATA SUBJECT – COMPLAINT TO THE SUPERVISORY AUTHORITY

By contacting the Company via email at **gdpr@cobogroup.net**, data subjects can request from the Data Controller access to their personal data, deletion of their data in the cases provided for by Art. 17 of the GDPR, rectification of inaccurate data, completion of incomplete data, restriction of processing in the cases provided for by Art. 18 GDPR, as well as opposition to processing, for reasons related to their particular situation, in cases of legitimate interest of the Data Controller.

Data subjects have the right to lodge a complaint with the competent Supervisory Authority in the Member State where they habitually reside, work, or where the alleged violation occurred.

Pursuant to Art. 2-undecies of Legislative Decree No. 196/2003, as amended by Legislative Decree No. 101/2018 (hereinafter, the "Code"), the rights under Articles 15 to 22 of the GDPR cannot be exercised if the exercise of such rights could result in actual and concrete prejudice to the confidentiality of the identity of the employee who reports unlawful conduct of which they became aware by virtue of their office.

In such cases, the rights in question may be exercised through the Data Protection Authority (in accordance with the procedures set out in Art. 160 of the Code), which will inform the data subject that all necessary verifications have been carried out or that a review has been conducted, as well as the data subject's right to lodge a judicial appeal.