

Curia Italy S.r.l.

I. Organizational Model ex. 231/2001 Legislative Decree

Curia Italy S.r.l. (“Curia Italy” or “the Company”) maintains, and updates annually, its Organizational Model, the current version of which has been in force since 2021. The Italian Legislative Decree 231 of 8 June 2001 introduced rules and regulations concerning the administrative responsibility of companies. These rules and regulations state that in certain circumstances the Company may be held responsible, and consequently be subject to fines for certain attempts to commit criminal offences, or for certain criminal offences actually committed, by the Company's directors and employees in the interests or to the advantage of the Company.

The Company is under the duty to adopt organizational, management and control procedures designed to prevent these offences. The principles of these procedures have been based on the code of practice (guidelines) established by Confindustria (Italian Manufacturers' Association).

The Company has a Surveillance Body (“Organismo di Vigilanza”), instituted with the task of keeping watch on the “Organizational, Management and Control Model Document” (the "Model") and its effective enforcement and updating, (a pivotal role in the Curia Italy legal compliance system). The Surveillance Body is formed by two members: one external to the organization (the Chairman) and one internal, both having appropriate professionalism and experience.

Once a year, the Board of Directors of Curia Italy S.r.l. reviews the recommendations of the Organismo di Vigilanza to ensure that the Model reflects the present organizational structure, and addresses newly introduced regulations.

In order to facilitate the collection of information, the Company has established the following information channels through which each employee and/or worker (also with a self-employed status) and/or officer and/or person belonging to the administrative, management or supervisory body and/or stakeholder and/or commercial partner may report illegal conduct under the Legislative Decree 231/2001 (as from time to amended and supplemented) and/or the Model and/or the Code of Ethics and Business Conduct (the “Code”):

1. ordinary or registered mail, sealed in a double envelope, to the attention of the mail address: Organismo di Vigilanza di Curia Italy S.r.l., Via del Politecnico 9, CAP 20122, Milan (MI), Italy;
2. an alternative channel operating by using IT-based methods, consisting of the following e-mail address: odv@curiaglobal.com;
3. a compliance hotline reachable at the following number: 800-78220, which operates also on IT-based methods at the following website: www.ethicspoint.com.

II. Information notice under the Legislative Decree 24/2023 (Italian transposition law of EU Directive 2019/1937 on the protection of persons who report breaches of Union law, the “Decree”)

Pursuant to article 5 of the Decree, the Company has established internal channels available to any persons below specified who acquired in a work-related context information on breaches of the Union law or other Italian laws affecting the public interest or the integrity of the Company:

- a) employees or persons having a self-employed status, including professionals and advisors;

- b) stakeholders and persons belonging to the administrative, management or supervisory board of the Company (including non-executive members and representatives), as well as volunteers, paid or unpaid trainees; and
- c) any persons working under the supervision and direction of contractors, subcontractors and suppliers.

The reporting persons qualify for protection under the Decree provided that they are in good faith, having reasonable grounds to believe that the information on breaches is true at the time of reporting and that such information falls within the scope of the Decree.

The internal channels below specified enable reporting in writing or orally, or both. Oral reporting will be possible by telephone or through other voice messaging system, and, upon request by the reporting person, by means of a physical meeting within a reasonable timeframe.

Internal reporting channels

- a) compliance hotline for oral reporting at the following number: 800-78220
- b) compliance helpline for written reports on IT-based methods at the following website: www.ethicspoint.com
- c) an alternative channel operating by using IT-based methods, consisting of the following e-mail address: odv@curiaglobal.com.

The processing of personal data disclosed by any reporting persons through the internal channels will be carried out in accordance with the Regulation EU 2016/679 (the “GDPR”) and Italian privacy laws. Personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, will be deleted. The identity of the reporting person, as well as any other information from which the identity of the reporting person may be directly or indirectly deduced, will be kept confidential, except where the disclosure is specifically permitted by the Decree and/or imposed by mandatory law provisions also with a view to safeguarding the rights of defence of the person concerned.

Any external report of breaches falling within the scope of the Decree will be possible according to article 7 et seq. of the Decree as soon as ANAC (“*Autorità Nazionale Anticorruzione*” the Italian anti-bribery authority) makes available its external reporting channel and related operative instructions (that you can check by clicking the link <https://www.anticorruzione.it/>), provided that at least one of the following requirements is met:

- internal reporting channels are not working properly or are not compliant with the Decree;
- the reporting person has first reported internally but no appropriate action was taken in response to the report;
- the reporting person has reasonable grounds to believe that in case of internal report no efficient follow-up would be provided, or the internal report would expose the reporting person to the risk of retaliation;
- the reporting person has reasonable grounds to believe that the breach may constitute an imminent or manifest danger to the public interest.