

pursuant to Art. 13 of EU Regulation 2016/679 (GDPR)



## CONTROLLER

Who decides the purposes and means of the processing?

Vinavil S.p.A. **is the data controller**, which means that it is the subject who determines the purposes and means of the processing of personal data pursuant to art. 4 of the GDPR. Below you can find the contact details of Mapei S.p.A.:

**Address:** Viale Jenner, 4 20159 - Milan Italy

**Telephone and Fax:** +39 02 695 541 e +39 02 69 55 48 90

**E-mail:** [privacy@vinavil.it](mailto:privacy@vinavil.it)

In the present information notice, Vinavil S.p.A. is also referred to as the **“Company”** or the **“Controller”**.

## What kind of data do we collect?

We collect personal data relating to **the reported person and the persons** mentioned in the report and, possibly, the **whistleblower** to fulfil the processing purposes listed in the following paragraph. Data are collected through the whistleblowing portal made available by the Company to report unlawful acts or omissions in breach of the Code of Ethics and the Organizational, Management and Control Model pursuant to Legislative Decree 231/2001 as well as of the Whistleblowing Policy (<https://www.vinavil.com/it/en/whistleblowing>) or through the channel made available to make oral reports.

Data provided by whistleblowers may concern the whistleblowers themselves (provided by the data subjects themselves pursuant to art. 13 GDPR) or the reported person or other persons (data provided by the whistleblower, therefore from a third party, pursuant to art. 14 GDPR).

Reports can be **non-anonymous or anonymous**. In case of non-anonymous reports, if the whistleblower so selects, the whistleblower may authorise the association of the whistleblower's personal data with the report. In case of anonymous reports, the IT systems of the Company **will not be able to identify the whistleblower** by the portal access point (IP address), even if the access occurs through a computer connected to the Company's network. To safeguard the investigation purposes on which the verification is based, the reported person may not be made aware of the processing of their data by the Controller until the report is considered grounded or significant evidence of its validity is collected. Such postponement will be assessed on a case-by-case basis by those in charge of the investigation together with the Controller, and taking into account the interest of evidence protection, in order to avoid its destruction or alteration.

In the context of a report, **common data and special categories** of data may be processed. Should the whistleblower make an oral report, collected data will include voice.



## PROCESSED DATA



## PURPOSES

### For what purpose do we process data?

The processing of the data is carried out for different purposes:

- 1. management of the reports on breaches of the Code of Ethics and/or the Organizational, Management and Control Model** pursuant to Legislative Decree 231/2001, including investigation activities to verify the validity of the reported facts and the adoption of the subsequent measures in accordance with the Model, as well as illicit conducts as defined in the Whistleblowing Policy;
- 2. ascertainment, exercise or defence of the Controller's rights** in court and/or in out-of-court procedures.

## What condition makes the processing lawful?

The processing must be founded on an adequate legal basis, to be lawful:

**1. compliance with a legal obligation** to which the Controller is subject (art. 6 D.Lgs. 231/2001 as amended by law 179/2017, requiring the Controller who has adopted a Model to make available specific channels to file reports) as well as EU Directive 2019/1937 implemented in Italy by D.Lgs. 24/2023), pursuant to art. 6, par. 1, lett. c) GDPR; with reference to oral reports, data will be processed with the prior consent of the data subject pursuant to art. 14 of D.Lgs. 24/2023; processing, if any, of special categories of data will be founded on the **carrying out the obligations and exercising specific rights** of the Controller and of the data subject in the field of employment law pursuant to art. 9, para. 2 lett. b) GDPR; any data on criminal convictions and offences will be processed only if authorised by law pursuant to art. 10 GDPR.

**2. legitimate interest of the Controller** or of a third party, pursuant to art. 6, par. 1, lett. f) GDPR and, in case of special categories of data, pursuant to art. 9, para. 2 lett. f) GDPR



## LEGAL BASIS

## How long do we retain personal data?



### RETENTION

We retain data for a period of time that varies according to the purpose of the processing:

- 1. for 10 years** from completion of the verification of the reported facts, **unless a judicial or disciplinary action is brought** against the reported person or the whistleblower who made false or defamatory declarations. In such a case data will be retained **for the entire duration of judicial or extrajudicial litigation**, until the time limits for appeals are exhausted, to the extent exceeding said 10-year term. Personal data related to **reports that are found ungrounded will be deleted within 2 months**;
- 2. for the entire duration of judicial or extrajudicial litigation**, until the time limits for appeals are exhausted. Once the above-mentioned retention periods have expired, data will be destroyed or anonymised, compatibly with the technical procedures of erasure and backup and with the Controller's accountability requirements.

## Is the provision of personal data necessary?

The provision of data marked with an asterisk (\*) is mandatory; in case of refusal to provide them, it will not be possible to process the report filed through the whistleblowing platform. The **provision of identity data of the whistleblower is optional**: in case of failure to provide them, the report will be validly processed in anonymous form.

Oral reports will be documented by means of recording on an appropriate storage device with the prior consent of the whistleblower: the whistleblower will be therefore requested to give such consent before collecting the report.



### NECESSARY



### THIRD PARTIES

## To whom could we communicate personal data?

The data may be communicated **to parties acting as data controllers**, such as, for example, authorities and supervisory and control bodies, individuals, companies, associations or professional firms providing assistance and consultancy.

Data are also processed by Mapei S.p.A. as data processor for the carrying out of supporting activities in the management and maintenance of the whistleblowing platform and storage of the information therein.

## Who is authorised to process the data?

Personal data may be processed by **the members of the dedicated team** who receive and manage reports in accordance with the Whistleblowing Policy. Such individuals have been expressly authorized to processing and provided with adequate operating instructions pursuant to art 29 GDPR and 2 quaterdecies D.Lgs. 196/2003 as amended by D.Lgs. 101/2018. For specific aspects of the report, or if deemed necessary, the support of other staff of the Company may be requested; such personnel will ensure that the absolute confidentiality is preserved



### AUTHORIZED



### EXTRA UE

## Can data be transferred to countries outside the EU?

**There will be no transfer of data outside the European Economic Area (EEA).**

## What are the data subject's rights?

By contacting the Company by e-mail at [privacy@vinavil.it](mailto:privacy@vinavil.it) data subjects may request access to the data concerning them, their **rectification, integration or deletion, the restriction of processing** in the cases provided for by Article 18 GDPR as well as **opposition to processing** in cases of legitimate interest of the data controller.

The exercise of said rights by the reported person may be limited due to the confidentiality obligations imposed on the Company by applicable law on the matter and to the necessity for the Company not to jeopardize the necessary investigations. In particular, rights under 15 to 22 GDPR cannot be exercised if their exercise may cause an effective and actual harm to the secrecy of the whistleblowing employee who reports, pursuant to law 2017/2019, an illicit conduct of which the whistleblower became aware by reason of office.

Finally, data subjects have the **right to lodge a complaint with the competent supervisory authority**.



### RIGHTS