



Information pursuant to Articles 13 and 14 of the European Regulation 2016/679 on the Processing of Personal Data in the Context of the Whistleblowing System of Dermaser S.r.l.

In compliance with current legislation (Legislative Decree 24/2023 - "Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and containing provisions regarding the protection of persons who report breaches of national regulations"), Dermaser S.r.l. (hereinafter also the "Company" or "Dermaser") has implemented a system for receiving and managing reports of alleged misconduct, allowing the management of the report ("Report") you submitted to the Company through specific dedicated channels.

The system is dedicated to receiving and managing Reports, including anonymous ones, submitted to the Company by company personnel and/or third parties concerning any violations of national or EU regulations, internal rules (conduct rules contained in the Code of Ethics, the 231 Model, and generally in the corporate regulatory framework), illegal conduct, and irregularities regarding the conduct of the Company's business activities.

Pursuant to Articles 13 and 14 of the European Regulation 2016/679 (hereinafter "GDPR"), the Company provides information on the processing of personal data ("Data") concerning you (as the "Whistleblower") acquired directly or otherwise in relation to the "Report" you submitted, as well as on the processing of the data of subjects affected by the Report itself (hereinafter also "Whistleblowing").

This information is made available and brought to the attention of potential interested parties through publication on the Company's institutional website.

The Company reserves the right, at its discretion, to change, modify, add or remove any part of this Information at any time.

Having said that, the Company provides below the information on the processing of personal data carried out in relation to the management of Reports as regulated by Dermaser's "Reporting Procedure".

1. DATA CONTROLLER

The Data Controller is Dermaser S.r.l. VAT No. 05140450965, with the following contact details:

- **Registered office:** Via Maurizio Gonzaga 7, Milan (MI) 20123;
- **PEC address:** dermaser@legalmail.it

The Data Controller has established the Supervisory Body appointed pursuant to art. 6, paragraph 1, letter b) of Legislative Decree no. 231/2001, endowed with autonomous initiative and control powers, which is also the owner of the whistleblowing process regulated by the "Reporting Procedure". Its members have been appointed as persons authorized to process personal data and have received adequate operational instructions.

To follow up on Reports, the Supervisory Body may use the support of internal/external personnel to the Company who will be identified and appointed as persons authorized to process personal data and will receive adequate operational instructions in this regard.

2. PURPOSES, LEGAL BASIS, AND OPTIONAL OR MANDATORY NATURE OF THE PROCESSING

Personal data are processed exclusively for the purposes of investigation and verification of the facts object of the Report and the adoption of any consequent measures according to Legislative Decree 24/2023.



In particular, the personal data collected are only those necessary and relevant to achieve the above purposes based on the "principle of minimization."

Concerning these data, their provision is voluntary, and the Interested Party is requested to provide only the data necessary to describe the facts subject of the Report without disclosing redundant and additional personal data beyond those necessary concerning the above purposes. If provided, the Data Controller will refrain from using such Data and will delete them.

Personal data are processed on the legal basis of the legal obligation ex art. 6, paragraph 1, letter b) (Legislative Decree 24/2023 – Legislative Decree 231/01) and the legitimate interest of the Data Controller ex art. 6, paragraph 1, letter f) of the GDPR (provided that the interests or fundamental rights and freedoms of the Interested Party do not prevail) to manage Reports of misconduct of which the Whistleblower has become aware for work-related reasons within their working context or for other reasons, and to protect the internal and external Interested Parties involved in the "Whistleblowing" procedure.

3. TYPES OF DATA PROCESSED

Within the "Whistleblowing" procedure, the personal data/information processed are the Data of the "Whistleblower" (or "Interested Party"), the "Reported" and the persons involved and/or connected to the facts object of the Report, such as, for example, any witnesses (hereinafter "Interested Parties").

These Data collected and processed by the Data Controller include "common" personal data of the Whistleblower/Interested Party, of the Interested Parties (personal details, job position held in the company, contacts such as: email address, postal address, phone number) and any other information present in your Report and possibly, in some cases where necessary, also data belonging to special categories ex art. 9 GDPR or data relating to criminal convictions and offenses ex art. 10 of the GDPR for reasons of significant public interest as per the Whistleblowing Decree and in any case within the limits allowed by the relevant legislation, including Articles 9 and 10 of the GDPR.

Data may be collected either directly from the Interested Party or through other subjects involved in the Report via the above-mentioned "internal reporting channel" or through other communication channels indicated in the continuation of this information notice.

The data are voluntarily provided by the Whistleblower/Interested Party, even anonymously, to the Data Controller, who will not process data that are not strictly necessary for the purposes.

By way of example and not exhaustive, the "Report" may be submitted by: employees of the Data Controller and/or third parties who have a relationship with the Data Controller.

4. METHODS OF PROCESSING

Data are collected in compliance with current regulations using electronic, telematic, and manual tools with logic strictly related to the above purposes, ensuring the security and confidentiality of the data themselves. In particular, they are collected through the following channels:

- The online platform "internal reporting channel" ex art. 4 Legislative Decree 24/2023 provided by a selected external provider that adopts a company misconduct reporting system compliant with Directive (EU) 2019/1937, guaranteeing the security and protection of data as well as the confidentiality of information through an advanced encryption system for communications and the database, in line with the relevant legislation. This platform allows the submission of Reports in written form, both anonymously and non-anonymously, and maintains interactions with the



Whistleblower and provides feedback on the Report within the timelines set by the regulations. The report is promptly managed by the Supervisory Body to ensure the case is handled in compliance with regulatory requirements;

- Sending an envelope containing the whistleblower's identification data and the Report to the Supervisory Body;
- Orally through a direct meeting with the Supervisory Body.

The data collected through electronic/telecommunication tools will not be subject to fully automated processing as specified in Article 22 of the GDPR. Specific security measures are in place to prevent data loss, illegal or improper use, and unauthorized access.

Additionally, specific technical-organizational measures, such as encryption, are adopted pursuant to Article 32 of the GDPR to ensure the protection of the identities of the data subjects, as well as the potential anonymity of the whistleblower and complete anonymity when accessing the platform (no log).

5. DATA RETENTION PERIODS

Personal data will be retained only for the time necessary to fulfill the purposes for which they are collected, in compliance with the principle of data minimization as per Article 5.1(c) of the GDPR. Specifically, this includes the time required for the investigation, conclusion of the whistleblowing process, and the adoption of relevant measures in case of confirmed violations. In any event, data will not be retained for more than 5 years from the date of communication of the final outcome of the whistleblowing procedure, in accordance with Article 14, paragraph 1 of Legislative Decree 24/2023 and Article 5, paragraph 1 of the GDPR.

6. DATA RECIPIENTS

If necessary for the investigation activities, some information related to the report may be processed by internal company functions that will be provided with specific instructions (e.g., functions responsible for investigations where their knowledge is indispensable for understanding the reported facts and/or for conducting the related investigation and/or handling activities).

These personal data related to the report may also be disclosed to the ANAC, judicial authorities, other competent entities/organizations in relation to the reported issue, and other external parties (e.g., consultancy firms, auditing firms, law firms, or entities providing services instrumental to the above purposes, limited to the information necessary for their assigned functions). This is necessary for investigation purposes, and the provider managing the operation and maintenance of the platform where reports can be submitted will be appointed as a "Data Processor" pursuant to Article 28 of the GDPR.

Under no circumstances will personal data be disseminated.

7. DATA SUBJECTS' RIGHTS

Articles 15-22 of the GDPR grant data subjects the ability to exercise specific rights, such as the right of access, rectification, erasure, and restriction of processing.

These rights can be exercised through a request made without formalities to the Data Controller at the PEC address provided.

The data subject may file a complaint with the Data Protection Authority pursuant to Article 57(f) of the GDPR.

If the exercise of the above rights by the reported person might cause real and concrete harm to the protection and confidentiality of the whistleblower's personal data, the Data Controller may limit, delay, or



deny such exercise, pursuant to Article 2-undecies, paragraph 1, letter f) of the Privacy Code (Legislative Decree 196/2003), and may not follow up on the request.

In such cases, the data subject's rights, pursuant to Article 2-undecies, paragraph 3 of the Privacy Code, can be exercised through the Data Protection Authority in accordance with the procedures set out in Article 160 of the Privacy Code.

8. POSSIBLE TRANSFER OF PERSONAL DATA TO NON-EU COUNTRIES

Personal data relating to the whistleblower, the reported person, or a third party will not be transferred to non-EU countries.

Saronno, 30/11/2023