

INFORMATION LETTER ON THE PROCESSING OF PERSONAL DATA

(articles 13 and 14 EU Reg. 2016/679 and Legislative Decree 196/2003 and subsequent amendments)

Dear,

Below we provide you with some information that you need to bring to your attention, not only to comply with legal obligations, but also because transparency and fairness towards interested parties is a fundamental part of our activity.

Who is the data controller?

The Data Controller of your personal data, responsible towards you for the legitimate and correct use of your personal data, is **PALLADIO GROUP S.P.A.**, which you can contact for any information or request at the following **contact details**:

Headoffice	Via Cresole n. 8, 36031 Dueville (VI), IT
Telephone	+39 0444 947111
E-mail	info@palladiogroup.com
Website	www.palladiogroup.com

N.B. The contact details for privacy communications of the Data Controller indicated above are not to be used for forwarding whistleblowing reports. For further details on the correct internal and external communication channels, on the prerequisites for making reports and on the procedure for their management, please refer to the documentation in the specific section of the Data Controller's website.

Who is the Data Protection Officer?

The Data Controller has appointed a Data Protection Officer (DPO) who can be contacted at the following contact details:

E-mail	dpo@palladiogroup.com
--------	-----------------------

N.B. The contact details of the DPO indicated above are not to be used for submitting whistleblowing reports. For further details on the correct internal and external communication channels, on the prerequisites for making reports and on the procedure for their management, please refer to the documentation in the specific section of the Data Controller's website.

Where is the data collected?

The data processed are communicated by the reporting party, as well as acquired independently by the Data Controller during any investigative activities that may become necessary, also by consulting public authorities and bodies and/or publicly accessible sources.

Is there an obligation to provide data?

The provision of personal data and other data useful for identifying the reporter is mandatory to

obtain a report pursuant to the Whistleblowing legislation (Legislative Decree 24/2023), while the provision of data other than the previous ones is optional. In case of failure to provide the mandatory data, the report will be considered anonymous and will be treated as indicated in the documentation present in the specific section of the Data Controller's website.

For what purposes are the data collected and processed?

The Data Controller collects and processes your personal data using automated, semi-automated and non-automated methods for purposes related to the management of the so-called whistleblowing reports, lawful on the basis of a legal obligation (Legislative Decree 24/2023). Any "special" data is processed for the fulfillment of obligations and the exercise of specific rights of the Data Controller or the Interested Party in matters of employment law. Any personal data relating to criminal convictions and crimes are processed for the fulfillment of obligations and the exercise of rights by the Data Controller or the interested party in matters of labor law or in any case in the context of employment relationships, within the limits established by laws, regulations and collective agreements. The table below shows the data processing analytically with details on the purpose, legal basis, type of data, specific recipients and cancellation terms.

To whom is the data communicated?

As part of the processing activities, your data may be communicated to:

- authorized subjects, as identified in the specific register kept by the Data Controller, including the whistleblowing manager;
- external parties who process the data on behalf of the Data Controller, duly instructed and bound through contracts of appointment as Data Processor (as identified in the specific register kept by the data controller), including the provider of the reporting channel (encrypted email) ;
- public authorities at their request or for communication obligations incumbent on the Data Controller (e.g. ANAC, judicial authorities, etc.).

N.B. It is specified that the identity of the reporting person and any other information from which such identity can be deduced, directly or indirectly, cannot be revealed without the expressed consent of the same to subjects or categories of subjects not mentioned above. In any case, the whistleblower is notified of the reasons for revealing the confidential data. Still on the subject, in the context of any criminal proceedings, the methods and limits established by the art 329 of the c.p.p. As part of the disciplinary proceedings, the identity of the whistleblower may be revealed, with the prior consent of the whistleblower, only if the dispute is based, in whole or in part, on the report or knowledge of the identity of the whistleblower is indispensable for the defense of the accused.

How is the data stored?

Your personal data is stored securely in compliance with the cancellation terms identified and reported below. However, consider that the data may be retained for the time necessary for the

statute of limitations to accrue in relation to mutual rights and the retention time of backups.

Are the data a subject to transfer?

If the whistleblower uses the reporting channel via encrypted email, the data will be transferred to Switzerland, where the provider of this channel is based, where transfer is lawful based on the adequacy decision by the European Commission. In other cases, the processing of personal data (e.g. storage, archiving and conservation of data on its own servers or in the cloud) is limited to the areas of circulation and processing of personal data of the countries belonging to the European Union, with express prohibition to transfer them to non-EU countries that do not guarantee (or in the absence of) an adequate level of protection, or, in the absence of protection tools provided for by EU Regulation 2016/679 (third country deemed adequate by the European Commission, BCR group, contractual clauses model, consent of interested parties, etc.). You can request further information by contacting the Data Controller.

Which rights can be exercised?

You are guaranteed the exercise of the rights recognized by the articles 15 ff. of the GDPR.

In particular, you are guaranteed, according to the methods and within the limits established by current legislation (see, for example, the provisions regarding whistleblowing in art. 2-undecies, paragraph 1, letter f) of the Legislative Decree 196/2003 as recently amended by Legislative Decree 24/2023, with effect from 15 July 2023), the exercise of the following rights:

- to request the Data Controller to access your personal data, as well as their rectification, cancellation or oblivion.
- to request data portability or limitation of processing;
- for reasons related to your particular situation, to oppose the processing based on legitimate interest of the personal data concerning you;
- for processing based on consent, to revoke consent at any time, without prejudice to the lawfulness of the processing based on the consent given before the revocation;
- to review the essential contents of any co-ownership agreements signed;
- to lodge a complaint with the Guarantor Authority for the protection of personal data, with headquarters in Piazza Venezia 11, 00187 – Roma – protocollo@pec.gdpd.it.

To exercise your rights or to request additional information, you can contact the Data Controller and/or the DPO, using the contact information above.

Can the information in this policy change?

The Data Controller may update this information on personal data in accordance with applicable laws. Any changes will be communicated appropriately and the update date will always be visible in the information. It is suggested that you regularly check the information and, if necessary, request an updated copy from the Data Controller.

Table A
What specific data processing operations are carried out?

Treatment	
Data processed	<p>The receipt and management of whistleblowing reports as per the procedure adopted by the Data Controller gives rise to processing of personal data known as "common" (personal data, contact data, address data, data relating to work activity, etc.), as well as giving rise, depending on the information spontaneously inserted in the report and in the deeds and documents voluntarily attached to it, to processing of personal data so-called "special" data (data relating to health conditions, trade union membership, etc., referred to in Article 9 GDPR) and personal data relating to criminal convictions and crimes (referred to in Article 10 GDPR).</p> <p>The data processed may concern the reporting subject, so-called whistleblower, the person or persons indicated as possibly responsible for the reported conduct, any other person named in the report or in the attached deeds and documents as well as anyone involved in various capacities in the procedure and events reported.</p> <p>Personal data that is clearly not useful for processing a specific report are not collected or, if collected accidentally, are deleted immediately.</p>
Purpose	<p>Manage the Whistleblowing reporting procedure as well as all the activities useful for receiving reports and their subsequent management, such as giving feedback to the whistleblowers regarding the receipt of the same, carrying out any investigative activities that may be necessary and adopting the consequent measures.</p>
Legal Basis	<p>Compliance with a legal obligation to which the Data Controller is subject. Any "special" data is processed for the fulfillment of obligations and the exercise of specific rights of the Data Controller or the Interested Party in matters of employment law;</p> <p>Any personal data relating to criminal convictions and crimes are processed for the fulfillment of obligations and the exercise of rights by the Data Controller or interested party in matters of labor law or in any case in the context of employment relationships, within the limits established by laws, regulations and collective agreements.</p>
Specific Recipients	<p>Manager of the so-called Whistleblowing reports Internal reporting channel provider (encrypted email)</p>
Storage	<p>For the time strictly necessary to implement the purpose and in any case no later than 5 years from the date of communication of the final outcome of the reporting procedure</p>