

Full Information – WHISTLEBLOWING

IGD SIIQ S.p.A., IGD Management SIIQ S.p.A., IGD Service S.r.l., Porta Medicea S.r.l. hereinafter the Joint Controllers, protect the confidentiality of your personal data and provides it with the necessary protection from any event that may put it at risk of violation.

For this purpose, the Joint Controllers implement policies and practices regarding the collection and use of personal data and the exercise of your rights under applicable law. The Joint Controllers are responsible for updating the policies and practices adopted for the protection of personal data whenever necessary and in any case in the event of regulatory and organisational changes that may affect the processing of your personal data.

The Joint Controllers appointed a Data Protection Officer (DPO) who you can contact if you have questions about adopted policies and practices. The contact details of the Data Protection Officer are as follows: dpo@gruppoigd.it

You can consult the Joint Controllers Agreement at the following link <http://www.gruppoigd.it/governance/etica-dimpresa/whistleblowing/>.

How does the Joint Controllers collect and process your data?

Your personal data (such as, name, surname, job title, place where you work, personal data collected by your report - e.g. date, place, modality and description of what happened) will be processed for the following purposes:

1) to fulfill and manage whistleblowing reports and consequent activities

Your personal data are processed by the Holding Company's Supervisory Body to fulfil its tasks. In particular, the processing will be aimed at ascertaining, through specific investigative activities, the validity of the report, with regard to the alleged wrongdoings reported in the interest of the integrity of the Joint Controllers.

Your personal data may also be processed by the Joint Controllers's Supervisory Bodies involved and by internal subjects authorised and trained in support of the ODV and, if the investigation is successful, may be communicated to the employer and to internal subjects for the purpose authorized in order to manage any proceedings resulting from the report and provided for by law or regulatory regulations (e.g. disciplinary measures).

The processing of your personal data is based on the fulfilment of legal obligations and the fulfilment of obligations arising from the existing relationship.

The provision of your personal data is necessary, the failure to issue implies that the Joint Controllers cannot carry out the verification activity.

2) for communication to recipients and/or third parties

In order to carry out all the processing activities necessary to pursue the purposes referred to in this policy, your personal data will be disclosed to the following third parties/recipients:

- Judicial Authorities or other Authorities/External Bodies.

The communication to these subjects takes place in compliance with specific legal obligations that the Joint Controllers expect through them. Any communication that does not fulfil these purposes will be subject to your consent.

The Joint Controllers will not transfer your personal data abroad (non-EEA countries). Your personal data will not be in any way disseminated or disclosed to undetermined and unidentifiable subjects, even as third parties.

3) for information security activities

Purposes	Legal bases
<ul style="list-style-type: none"> - control and monitoring of the services displayed on the network and on the platforms belonging to the Joint Controllers and made available to you also because of the activities carried out on behalf of the Joint Controllers (access to the Platform, administration of the systems in use, etc.) - Implementation of procedures for the detection and notification of personal data breaches (Data Breach) 	<ul style="list-style-type: none"> Fulfillment of activities dependent on the relationship established Fulfillment of legal obligations (detection and notification of Data Breach events) Legitimate interest

How and for how long are your data stored?

Data processing is carried out on paper or through IT procedures by internal subjects authorised and trained for this purpose. They are granted access to your personal data to the extent and within the limits required for carrying out the processing activities that concern you.

The Joint Controllers periodically check the tools by means of which your data is processed and its security measures, which it constantly updates; it makes sure, also through the subjects authorised to process the data, that personal data for which processing is not necessary is not collected, processed, stored or retained; it makes sure that the data is retained with the guarantee of integrity and authenticity of its use for the purposes of the processing actually carried out.

Personal data are also stored in electronic archives protected by effective and adequate security measures to counter the risk of infringement considered by the Joint Controllers for the time necessary to comply with the required assessment and in any case not over 30 days, if the report is unfounded, or five years from the closure of the investigation for the handling of any complaints, unless internal disciplinary proceedings or litigation are instituted for as long as is necessary for the defence in court and as a result. Once all the purposes that legitimize the storage of your personal data have been exhausted, the Joint Controllers will take care to delete them or make them anonymous.

What are your rights?

Consistent with the time limits established for the processing of your personal data, the rights you are granted allow you to always have control of your data. Your rights are:

- access;
- rectification;
- erasure;
- restriction of processing;
- objection to processing;
- portability.

Your rights are guaranteed without any special charges or formalities: the request to exercise them is essentially free of charge. You have the right:

- obtain confirmation of the processing carried out by the Joint Controllers;
- access your personal data and know its origin (when the data is not obtained directly from you), the purposes of the processing, the data of the subjects to whom it is communicated, the period of retention of your data or the criteria used to determine it;
- withdraw your consent at any time if this is the basis for the processing. In any case, the withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal;

- update or rectify your personal data so that it is always accurate and correct;
- erase your personal data from the databases and/or files, including backup files, of the Joint Controllers, if, among other things, it is no longer necessary for the purposes of the processing or if this is deemed unlawful, and provided that the conditions laid down by law are met; and in any event if the processing is not justified by another equally legitimate reason;
- restrict the processing of your personal data in some circumstances, for example if you have contested its accuracy, for the period required for the Joint Controllers to check its accuracy. You must also be informed, in reasonable time, of when the period of suspension has ended or the cause of the restriction of processing has ceased to exist, and therefore the restriction itself withdrawn;
- obtain your personal data, if received and/or in any case processed by the Joint Controllers with your consent and/or if its processing is carried out on the basis of a contract and with automated tools, in electronic format also in order to transmit it to another data controller.

The Joint Controllers must do so without delay and, in any case, at the latest within one month of receipt of your request. The time limit can be extended by two months, if necessary, taking into account the complexity and the number of requests received by the Joint Controllers. In such cases, the Joint Controllers will inform you of the reasons for the extension within one month of receipt of your request.

For any further information and to send your request, please contact the Joint Controllers at privacy@gruppoigd.it

How and when can you oppose the processing of your personal data?

For reasons relating to your specific situation, you may oppose at any time the processing of your personal data if this is based on legitimate interest, by sending your request to the Joint Controllers at the email address privacy@gruppoigd.it

You have the right to have your personal data erased if there is no legitimate reason overriding the one that gave rise to your request.

Who can you complain to?

Without prejudice to any other administrative or judicial action, you may submit a complaint to the competent supervisory authority or to the authority that carries out its tasks and exercises its powers where you have your habitual residence or work or, if different, in the Member State where the violation of Regulation (EU) 2016/679 occurred.

Any update of this information will be communicated to you in a timely manner and by appropriate means and you will also be informed if the Joint Controllers will process your data for purposes other than those referred to in this information before carrying it out and in time to give your consent if necessary.