

PERSONAL DATA PROCESSING POLICY WHISTLEBLOWER

Articles 13 and 14 of Regulation (EU) 2016/679 – GDPR

HEXPOL Garlasco S.r.l. (the "Data Controller") – in compliance with the provisions of EU Regulation 2016/679 ("GDPR") – intends to provide you with specific information on the processing of personal data that is necessary in relation to reports of illegal activities or irregularities submitted via the *whistleblowing* portal (hereinafter the "Portal") or via other reporting channels made available by the Data Controller (post and/or meeting).

1. IDENTITY AND CONTACT DETAILS OF THE DATA CONTROLLER AND DATA PROTECTION OFFICER

- The Data Controller is HEXPOL Garlasco S.r.l., with registered office in Garlasco (PV) – 27026, at Via Borgo San Siro 66, and can be contacted at the following email address: info.gar@hexpol.com

The Data Controller has appointed a Data Protection Officer who can be contacted at the following email address: dpo@c2compliance.it

2. DATA SUBJECTS

The Portal is made available to the following categories of data subjects ("*identified or identifiable natural persons*"):

- Employees, including managers, full-time and permanent
- External collaborators and freelancers
- Members of the Board of Directors and Supervisory Board
- Paid and unpaid trainees and interns

(individually **the "Data Subject"**, collectively the "Data **Subjects**")

In cases where the report is made by a person who has an employment or collaboration relationship with the Company, this shall be understood as supplementary to the information provided to the Data Subject for the management of the relationship.

3. DATA SUBJECT TO PROCESSING

The data collected and processed includes the personal details and contact details of the reporting person, if they decide to provide them, data relating to the employment relationship, the role performed, or the elements characterising the report ("**Common Data**").

The Data Controller will process data belonging to special categories, i.e. data revealing, among other things, racial and ethnic origin, data relating to health and sex life ("**Special Data**") only if you freely decide to provide them as elements characterising the report.

The Data Controller may also process **Data relating to criminal convictions and offences** if they are the subject of the report.

Common Data and Special Data relating to criminal convictions and offences are hereinafter collectively referred to as "**Personal Data**".

Personal Data may also concern the reported person, the facilitator, people in the same work environment and work colleagues of the reporting person.

Personal Data is provided directly by you by filling in the appropriate fields and/or can be obtained from the report (whether written or oral), subsequently, if you decide to add further details to the report via the Portal's messaging system, which allows you to establish a virtual conversation with the body responsible for handling the report.

4. PURPOSE OF THE PROCESSING AND LEGAL BASIS

Pursuant to the Privacy Regulation, the processing of personal data must be legitimised by one of the various legal conditions set out in Articles 6, 9 and 10 of the GDPR. These conditions are expressly indicated below for each purpose for which the Data Controller processes your data:

- Fulfilment of legally binding obligations : Personal Data and information will be processed to ensure the complete and correct management of the whistleblowing procedure, including preliminary investigations necessary to verify the facts reported and take the appropriate measures.

Legal basis for processing: Personal Data is collected and processed for the fulfilment of a legal obligation to which the Data Controller is subject (*Art. 6(1)(c) GDPR*), namely the management of the *whistleblowing* procedure, in accordance with the provisions of Legislative Decree 24/2023 implementing '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 laying down provisions on the protection of persons who report breaches of national law' and in accordance with Art. 10 GDPR, as data relating to criminal convictions and offences may be processed.

- Defence in court for the rights of the Data Controller: Where required, Personal Data and information will be disclosed to the authorities responsible for law enforcement.

The Data Controller reserves the right to process Personal Data and information to defend and/or protect its rights in court.

Legal basis for processing: Personal Data is collected and processed on the basis of the legitimate interest of the Data Controller (Article 6(1)(f) of the GDPR) for the fulfilment of the specific procedure relating to Model 231.

- Use of the report for defence purposes in disciplinary proceedings: Personal Data may be disclosed to persons other than those competent to receive or follow up on reports, in the context of disciplinary proceedings where the disciplinary charge is based on separate and additional findings to the report, even if consequential to it. Personal Data may be disclosed if the charge is based, in whole or in part, on the report and knowledge of the identity of the reporter is essential for the defence of the accused.

Legal basis for processing: Personal Data is processed on the basis of your specific consent (Articles 6(1)(a) and 9(2)(a) of the GDPR), which you may give directly online, before submitting the report on the Portal, or during an interview. The report will only be used for disciplinary proceedings if consent is given.

5. RETENTION PERIOD

The data is processed and stored for the entire duration of the whistleblowing procedure, including the time required to carry out any proceedings arising from the management of the report. At the conclusion of the last proceeding, the data is stored for a further 5 years. This is without prejudice to storage for a longer period in cases where this is necessary in relation to requests from public authorities or for the exercise of the Data Controller's right of defence.

6. CATEGORIES OF RECIPIENTS OF PERSONAL DATA AND TRANSFER

The data may be disclosed to third parties whose knowledge is necessary for the performance of the report management activities and/or to external parties acting as Data Processors pursuant to Article 28 of the GDPR.

The data may also be disclosed to internal staff, where necessary for the purposes of verifying the validity of the report and any consequent actions.

Personal Data will not be disclosed in any way.

7. METHOD OF PROCESSING

The data will be processed, recorded and stored using both electronic and paper-based tools, through the adoption of appropriate technical and organisational measures pursuant to Article 32 of the GDPR, such as to guarantee its security and confidentiality. The Personal Data of the Data Subject may be processed by personnel of the Data Controller who are expressly authorised to do so and who have received adequate operating instructions pursuant to and for the purposes of Article 29 of the GDPR.

The Portal applies encryption techniques to data, both in transit and stored. Paper documentation and any records are limited to the minimum necessary and stored in cabinets and rooms equipped with security locks.

8. DATA TRANSFER TO NON-EU COUNTRIES

The data provided by the Data Subject will be processed within the European Union. In the event that transfer to countries outside the EU becomes necessary, compliance with the applicable legal provisions, as set out in Articles 44 et seq. of the GDPR, will be guaranteed.

9. RIGHTS OF THE DATA SUBJECT

Pursuant to current legislation (Articles 15 et seq. of the GDPR), the data subject may exercise the following rights:

- a. access: the possibility of obtaining confirmation from the Data Controller as to whether or not Personal Data is being processed and, if so, to obtain access to the data itself;
- b. rectification: to correct/obtain the correction of Personal Data if it is incorrect or obsolete and to complete it if it is incomplete;
- c. erasure/right to be forgotten: to obtain the erasure of the Personal Data provided, except in cases where the Data Controller has legitimate or legal reasons for retaining it;
- d. restriction: the data will be retained by the Data Controller, but will not be processed or further processed in the cases provided for by law;
- e. portability: the possibility of obtaining a copy of one's data to transfer it to another Data Controller, only for data provided by the data subject and in cases where the processing is based on consent and carried out by automated means;
- f. objection: the possibility of objecting to the processing of one's data, without prejudice to the Data Controller's right to demonstrate the existence of legitimate reasons for proceeding anyway;
- g. withdrawal of consent at any time, if the processing is based on consent.

The exercise of the data subject's rights may be delayed, limited or excluded, with reasoned notification given without delay, unless the notification could compromise the purpose of the limitation, for as long as and to the extent that this constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the Data Subject, in order to safeguard the confidentiality of the identity of the employee who reports offences of which he or she has become aware (Article 2-undicies, paragraph 1, letter f) of Legislative Decree 196/2003). In such cases, the rights of the data subject may also be exercised through the Data Protection Authority in accordance with the procedures set out in Article 160 of the same Decree. In this case, the Data Protection Authority shall inform the data subject that it has carried out all the necessary checks or has conducted a review, as well as of the data subject's right to seek judicial review.

The exercise of rights must be carried out through the same channel used for the report or by sending an email to: dpo@c2compliance.it

The Data Controller will respond within 30 days of receiving the formal request sent by the Data Subject.

The data subject has the right to lodge a complaint with the supervisory authority of the Member State in which they reside or work, or of the State in which the alleged infringement occurred.

The reported person and/or other persons mentioned in the report may not exercise the above rights for as long as and to the extent that this constitutes a necessary and proportionate measure, pursuant to Article 2-*undecies* of Legislative Decree 196/2003 and subsequent amendments and additions, as the exercise of such rights could result in actual and concrete prejudice to the protection of the confidentiality of the identity of the reporting person.