FORGING GROUP MONALE S.r.l.
SEDE AMMINISTRATIVA E OPERATIVA:
Str. Castellero 18/20 – 14013 Monale d'Asti – AT – Italy
SEDE LEGALE:
Via Legnano 26 – 10128 Torino – TO
Tel.: +39 0141 / 669819 – Fax: +39 0141 / 669800
PIVA/CF: 10108770016

WHISTLEBLOWING PRIVACY NOTICE

pursuant to Articles 13 and 14 of Regulation (EU) 2016/679 ("GDPR"), Article 13 of Legislative Decree No. 24/2023 (the "Whistleblowing Decree", implementing Directive (EU) 2019/1937) and Legislative Decree No. 196/2003 (the "Italian Privacy Code")

Forging Group Monale S.r.l. (hereinafter also "F.G.M." or "the Company") has set up an internal reporting channel which makes it possible to report, confidentially or anonymously, breaches of national or European Union law and of the Organisation, Management and Control Model pursuant to Legislative Decree No. 231/2001 ("Model 231") that have come to one's knowledge in a work-related context, as provided for by Legislative Decree No. 24/2023. With this document, F.G.M. explains, in a simple and transparent way, how the personal data contained in reports are processed and what protections are guaranteed to the persons involved. The operating procedures for submitting a report are described in the Company's Whistleblowing Procedure.

1. DATA CONTROLLER

The Data Controller, i.e. the entity that decides why and how the data are processed (Article 4(7) GDPR), is:

- **Forging Group Monale S.r.l.** – VAT No./Tax Code 10108770016
- Registered office: Via Legnano 26, 10128 Turin (TO), Italy
- Administrative and operational headquarters: Str. Castellero 18/20, 14013 Monale d'Asti (AT), Italy
- Tel.: +39 0141 669819 – Certified e-mail (PEC): forging-group@legalmail.it – e-mail for privacy matters: alessandra.madonna@forging-group.com.

2. DATA PROTECTION OFFICER (DPO)

F.G.M. has not appointed a Data Protection Officer (DPO), as the conditions making such an appointment mandatory under Article 37 GDPR do not apply to it. For any matter relating to personal data, you may contact the Data Controller directly using the contact details given in section 1.

3. WHO THIS NOTICE IS ADDRESSED TO

This notice concerns all persons whose data may be processed in connection with a report (hereinafter the "**Data Subjects**"), and in particular:

- the **person making the report** (the "**Reporting Person**"): employees, collaborators, self-employed workers, freelance professionals, consultants, volunteers, trainees, shareholders, members of corporate bodies, as well as workers and collaborators of F.G.M.'s customers and suppliers (Article 3 of Legislative Decree No. 24/2023), including during the probationary period, before the relationship begins or after it has ended;
- the **person concerned** (the "**Person Concerned**"), i.e. the person to whom the breach is attributed or who is otherwise implicated in the report;
- the **facilitator**, i.e. the person who assists the Reporting Person in the reporting process, and the **other persons mentioned** in the report (e.g. witnesses, colleagues, family members).

The data of the Person Concerned and of the other persons mentioned are obtained through the Reporting Person (Article 14 GDPR). In order not to jeopardise the investigation of the facts and the confidentiality of the Reporting Person, information to the Person Concerned may be provided at a later stage or be limited, in the cases provided for by Article 14(5)(b) GDPR and Article 2-undecies of the Italian Privacy Code.

4. REPORTING CHANNELS AND HOW DATA ARE COLLECTED

Reports can be made through the following internal channels (Article 4 of Legislative Decree No. 24/2023):

- **dedicated IT platform**, provided by Whistleblower Software ApS and available at whistleblowersoftware.com/secure/Forging-group (also linked from the "Whistleblowing" page of the Company website). This is the recommended channel: communications are encrypted and the platform allows reports to be made anonymously as well, and to communicate with the report handler without revealing one's identity;
- **in writing on paper**, delivered in the manner set out in the Whistleblowing Procedure (e.g. in a sealed envelope marked "confidential – for the attention of the report handler");
- **orally**, at the request of the Reporting Person, through a face-to-face meeting with the report handler. With the Reporting Person's consent, the meeting is documented by means of a recording or minutes, which the Reporting Person may check, correct and confirm by signing them (Article 14(2) and (4) of Legislative Decree No. 24/2023).

Further data may be collected while the report is being handled and during the investigation needed to verify whether it is well-founded. In addition, the Company network security systems (firewall) may record connection logs to the platform when it is accessed from Company devices or networks. For maximum confidentiality, we recommend accessing the platform from a personal device and a non-Company network.

This is without prejudice to the possibility of submitting an external report to ANAC (the Italian National Anti-Corruption Authority) and to the other forms of reporting provided for by Articles 6 and 15 of Legislative Decree No. 24/2023, under the conditions laid down by law. In such cases ANAC acts as an independent data controller.

5. WHAT DATA WE PROCESS

In compliance with the data minimisation principle (Article 5(1)(c) GDPR), the following data may be processed:

- in the case of a **non-anonymous** report, the identification and contact data of the Reporting Person (e.g. first name, surname, e-mail address, telephone number) and his or her role in or relationship with the Company;
- the data of the Person Concerned and of the other persons mentioned, to the extent that they are contained in the report;
- the facts reported and any other information or document attached to the report or emerging during the investigation;
- any special categories of personal data (Article 9 GDPR, e.g. health data) and data relating to criminal offences (Article 10 GDPR), only if contained in the report and strictly necessary for handling it;
- the technical data of the connection logs referred to in section 4.

Data that are manifestly not useful for processing a specific report are not collected or, if collected accidentally, are deleted immediately (Article 13(2) of Legislative Decree No. 24/2023). Anonymous reports are handled in the same way as other reports, if sufficiently detailed; if the

anonymous Reporting Person is subsequently identified and suffers retaliation, he or she benefits from the protections provided for by law.

6. WHY WE PROCESS THE DATA, LEGAL BASIS AND RETENTION PERIOD

The GDPR allows personal data to be processed only if there is a valid "legal basis" (Articles 6, 9 and 10 GDPR). The following table shows, for each purpose, the legal basis applied and the retention period.

Purpose of processing	Legal basis	Retention
A. Receipt and handling of reports Receiving reports, communicating with the Reporting Person, carrying out the investigation to verify whether the facts are well-founded, providing feedback to the Reporting Person and adopting the resulting measures, also for the effective implementation of Model 231.	Legal obligation (Article 6(1)(c) GDPR) – Legislative Decree No. 24/2023 and Legislative Decree No. 231/2001 Employment law (Article 9(2)(b) GDPR) Data relating to criminal offences: Article 10 GDPR and Article 2-octies of the Italian Privacy Code	For the time necessary to handle the report and in any case **no longer than 5 years** from the communication of the final outcome (Article 14(1) of Legislative Decree No. 24/2023).
B. Disciplinary proceedings and protection of rights Initiation of any disciplinary proceedings resulting from the report; establishment, exercise or defence of a right of the Data Controller in court.	Legal obligation (Article 6(1)(c) GDPR) Legitimate interest (Article 6(1)(f) GDPR) Legal claims (Article 9(2)(f) GDPR)	5 years as above or, if later, until the final conclusion of the disciplinary or judicial proceedings.
C. Disclosure of the Reporting Person's identity Disclosing the identity of the Reporting Person to persons other than the report handler, where this is essential (e.g. for the defence of the Person Concerned in disciplinary proceedings).	**Express consent** of the Reporting Person (Article 6(1)(a) GDPR; Article 12(2) and (5) of Legislative Decree No. 24/2023)	As for purpose A.
D. Requests from the Authorities Responding to requests from the judicial authorities, ANAC or other competent Authorities.	Legal obligation (Article 6(1)(c) GDPR)	For the time necessary to follow up on the request.
E. IT security Management of Company network security, including connection logs to the platform, exclusively for the resolution of IT incidents.	Legitimate interest in ensuring network security (Article 6(1)(f) and Recital 49 GDPR)	For the period set out in the Company's Data Retention Policy.

Recorded oral reports and the related minutes are subject to the same retention periods. At the end of the periods indicated, the data are deleted or anonymised.

7. CONFIDENTIALITY OF THE REPORTING PERSON'S IDENTITY

The identity of the Reporting Person and any other information from which it may be inferred, directly or indirectly, may not be disclosed without his or her express consent to persons other than those competent to receive or follow up on reports, who are expressly authorised to process the data (Article 12(2) of Legislative Decree No. 24/2023). In particular:

- in disciplinary proceedings, if the charge is based on investigations that are separate from and additional to the report, the identity of the Reporting Person may not be disclosed. If the charge is based, in whole or in part, on the report and knowledge of the identity is

essential for the defence of the Person Concerned, the report may be used only with the express consent of the Reporting Person (Article 12(5));

- in these cases, the Reporting Person receives a written notice setting out the reasons why it is necessary to disclose his or her identity (Article 12(6));
- the same confidentiality is guaranteed for the identity of the Person Concerned, the facilitator and the persons mentioned, until the conclusion of the proceedings initiated as a result of the report (Article 12(7));
- the Reporting Person is protected against any form of retaliation resulting from the report (Article 17 of Legislative Decree No. 24/2023).

8. WHETHER PROVIDING DATA IS MANDATORY

Providing the identification data of the Reporting Person is optional: reports can also be made anonymously. However, a report must contain sufficiently detailed information to allow the facts to be verified; otherwise, it may not be possible to follow it up.

9. PROCESSING METHODS AND SECURITY MEASURES

The data are processed mainly by IT means, through the dedicated platform, in accordance with the Whistleblowing Procedure, only by specifically authorised and instructed persons (Article 29 GDPR and Article 2-quaterdecies of the Italian Privacy Code). Pursuant to Article 32 GDPR and Article 13(6) of Legislative Decree No. 24/2023, F.G.M. adopts appropriate technical and organisational measures to ensure the confidentiality of Reporting Persons, of the other persons involved and of the content of reports, including:

- encryption of communications and of data stored on the platform;
- access to reports restricted to the report handler only, through personal credentials;
- the possibility of reporting anonymously and of communicating with the report handler without revealing one's identity;
- storage of paper documents in archives accessible only to the report handler;
- consultation of connection logs only by authorised technicians and exclusively for the resolution of IT incidents, after informing the Data Controller.

F.G.M. does not use automated decision-making, including profiling (Article 22 GDPR).

10. TO WHOM THE DATA MAY BE DISCLOSED

The data are not disseminated. They may be accessed, only for the purposes stated and to the extent necessary, by:

- the report handler identified in the Whistleblowing Procedure (Article 4 of Legislative Decree No. 24/2023), who acts as a person authorised to process the data or, if external to the Company, as a data processor (Article 28 GDPR);
- Whistleblower Software ApS, the platform provider, appointed as data processor (Article 28 GDPR);
- the Supervisory Body (Organismo di Vigilanza) pursuant to Legislative Decree No. 231/2001, for reports concerning Model 231;
- the Company functions responsible for adopting the resulting measures (e.g. disciplinary proceedings), without disclosing the identity of the Reporting Person unless he or she gives express consent;
- legal advisers, the judicial authorities, ANAC and other competent Authorities, in the cases provided for by law.

11. TRANSFER OF DATA OUTSIDE THE EUROPEAN UNION

F.G.M. does not transfer report data to countries outside the European Union: the platform stores data on servers located in the EU. Should a transfer become necessary, it will take place only to countries covered by an adequacy decision (Article 45 GDPR) or on the basis of appropriate safeguards, such as the Standard Contractual Clauses (Article 46 GDPR), and this notice will be updated.

12. RIGHTS OF DATA SUBJECTS

Data Subjects may exercise the following rights (Articles 15 to 22 GDPR), subject to the limitations set out below the table:

Right	Reference	In practice
Access	Art. 15 GDPR	To know whether we process data concerning him or her and, if so, to obtain a copy of them and to know the purposes, categories of data, recipients and retention period.
Rectification	Art. 16 GDPR	To have inaccurate data corrected or incomplete data completed.
Erasure ("right to be forgotten")	Art. 17 GDPR	To have the data deleted, unless retention is necessary to comply with legal obligations or for the defence of legal claims.
Restriction	Art. 18 GDPR	To have the data only stored, without any further use, for example while their accuracy is being verified.
Objection	Art. 21 GDPR	To object, on grounds relating to his or her particular situation, to processing based on legitimate interest (purposes B and E), unless the Data Controller has compelling legitimate grounds or needs to defend legal claims.
Withdrawal of consent	Art. 7(3) GDPR	The Reporting Person may withdraw consent to the disclosure of his or her identity (purpose C), without affecting the lawfulness of processing already carried out.
Automated decisions	Art. 22 GDPR	Not to be subject to decisions based solely on automated processing. F.G.M. does not carry out such processing.
Complaint	Art. 77 GDPR	To lodge a complaint with the Italian Data Protection Authority – Garante per la protezione dei dati personali (Piazza Venezia 11, 00187 Rome, Italy – www.garanteprivacy.it) or with the supervisory authority of the EU Member State in which he or she lives or works.

Limitations of rights. Pursuant to Article 13(3) of Legislative Decree No. 24/2023 and Article 2-undecies(1)(f) of the Italian Privacy Code, the above rights may not be exercised, or may be delayed or restricted, if their exercise could result in actual and concrete harm to the confidentiality of the Reporting Person's identity. This applies in particular to the Person Concerned, who may not obtain, for example through the right of access, information that would make it possible to identify the Reporting Person. The limitation is communicated to the Data Subject with the reasons for it, unless this would undermine the purpose of the limitation, and is applied for as long as and to the extent that it constitutes a necessary and proportionate measure. In these cases, the Data Subject may ask the Garante to carry out the necessary checks (Article 2-undecies(3) and Article 160 of the Italian Privacy Code).

13. HOW TO EXERCISE YOUR RIGHTS

Requests can be sent:

- by e-mail to: alessandra.madonna@forging-group.com;

- by certified e-mail (PEC) to: **forging-group@legalmail.it**;
- or by registered letter with return receipt to: Forging Group Monale S.r.l., Str. Castellero 18/20, 14013 Monale d'Asti (AT), Italy.

A Reporting Person who has submitted a report through the platform may also make the request through the platform's confidential messaging area, without revealing his or her identity to anyone other than the report handler. The Data Controller will reply **within one month** of receipt of the request, which may be extended by **two further months** where requests are complex or numerous (Article 12(3) GDPR). Exercising these rights is **free of charge**, except in the case of manifestly unfounded or excessive requests (Article 12(5) GDPR).

14. UPDATES TO THIS NOTICE

This notice (Issue 2) replaces the previous issue of 12 December 2023 and may be updated in the event of regulatory or organisational changes. The version in force is published on the "Whistleblowing" page of the Company website and is available at F.G.M.'s premises.

Monale d'Asti, 8 October 2026

The Data Controller
Forging Group Monale S.r.l.