



PRIVACY POLICY

*on the processing of personal data of individuals submitting
reports through My Whistleblowing 2.0*



PRIVACY POLICY

PERSONAL DATA AND PRIVACY

Pursuant to Articles 13 and 14 of Regulation (EU) 2016/679 ("GDPR") and Article 13 of Legislative Decree No. 196/2003 (the "Privacy Code"), we hereby provide you with this Privacy Notice.

DATA CONTROLLER

The Data Controller is AMA S.p.A., with registered office at Via Puccini, 28 42018 San Martino in Rio, Reggio nell'Emilia, Italy, email address: privacy@ama.it.

PLACE OF DATA PROCESSING

Processing activities related to the management of whistleblowing reports are carried out in Italy. No transfer or disclosure of personal data to third countries or international organisations takes place.

No personal data shall be disclosed or communicated to third parties, except where required by law or where necessary for the handling of the report and compliance with applicable legal obligations.

PURPOSES OF THE PROCESSING

The personal data provided are processed exclusively for the receipt, assessment, handling and follow-up of whistleblowing reports, as well as for compliance with the obligations set out in Legislative Decree No. 231/2001 and Legislative Decree No. 24/2023.

Per una formulazione più conforme al linguaggio GDPR anglosassone, suggerisco di utilizzare "assessment" e "follow-up of whistleblowing reports", termini comunemente impiegati nelle privacy notice relative ai sistemi whistleblowing. Inoltre, il titolo del documento dovrebbe preferibilmente essere "Privacy Notice" anziché "Privacy Policy".

CATEGORIES OF PERSONAL DATA PROCESSED

The personal data processed may include:

- ✓ identification data of the Reporting Person (name, surname, contact details);
- ✓ data relating to the report (reported facts, individuals involved, supporting documentation attached);
- ✓ any other personal data that may be contained in the report.

The Reporting Person is requested to provide only data that is relevant and strictly necessary for the purposes of the report. Information that is manifestly irrelevant may not be taken into consideration or may be deleted.

LEGAL BASIS FOR THE PROCESSING

The legal basis for the processing is the compliance with legal obligations to which the Data Controller is subject, pursuant to Article 6(1)(c) of the GDPR, in particular:



- ✓ Article 6 of Legislative Decree No. 231/2001;
- ✓ Legislative Decree No. 24/2023 implementing Directive (EU) 2019/1937;
- ✓ any other applicable whistleblowing laws and regulations.

DATA RETENTION PERIOD

Personal data will be retained for the time necessary to manage the report and, in any event, no longer than the retention periods prescribed by applicable law.

In accordance with Article 14 of Legislative Decree No. 24/2023, documentation relating to whistleblowing reports shall be retained for the time necessary to process the report and, in any case, for no longer than five years from the date of communication of the final outcome of the reporting procedure.

Personal data that is manifestly not relevant to the processing of a specific report shall not be collected or, if inadvertently collected, shall be deleted without undue delay.

WE SHARE THE COLLECTED DATA WITH

Personal data may be accessed only by:

- ✓ persons specifically authorized to manage whistleblowing reports;
- ✓ members of the Supervisory Body pursuant to Legislative Decree No. 231/2001, where involved;
- ✓ consultants and professionals who may be involved in the investigation process, to the extent necessary;
- ✓ the provider of the IT platform used for managing reports, appointed as a Data Processor pursuant to Article 28 of the GDPR.

Personal data shall be shared in compliance with the principles of necessity, data minimization and confidentiality.

METHODS OF PROCESSING

Personal data is processed by means of electronic and paper-based tools and through procedures designed to ensure its security, integrity, availability and confidentiality.

Specific technical and organizational measures are implemented to prevent data loss, unlawful or unauthorized use and unauthorized access.

ANONYMOUS REPORTS AND GOOD FAITH OF THE REPORTING PERSON

The Data Controller recognizes the possibility of submitting anonymous reports, provided that they are sufficiently detailed and comply with applicable laws and internal procedures.



Reports must be submitted in good faith and on the basis of reasonable grounds to believe that the information reported is true and accurate. Any civil, criminal, or disciplinary liability provided for by law in cases of proven slander, defamation, or reports made with wilful misconduct or gross negligence shall remain unaffected.

The persons responsible for handling reports may decide to close reports that are manifestly unfounded, generic, lacking sufficient elements to verify the facts, or falling outside the scope of whistleblowing legislation, in accordance with applicable internal procedures and legal requirements.

The Reporting Person is requested to provide only data and information that are relevant and strictly necessary for the purposes of the report.

DATA SUBJECTS' RIGHTS

Under certain conditions, data subjects may exercise the rights provided for under Articles 15 to 22 of the GDPR, including:

- ✓ access to personal data;
- ✓ rectification of inaccurate data;
- ✓ deletion of data in the cases provided for by law; restriction of processing; objection to processing in permitted cases;
- ✓ data portability where applicable;
- ✓ withdrawal of consent,
- ✓ where the processing is based on consent.

The exercise of the above rights may be restricted in cases provided for by applicable law and, in particular, where the exercise of such rights could result in actual prejudice to the confidentiality of the Reporting Person's identity or to the conduct of assessment and investigation activities carried out under whistleblowing legislation.

To exercise these rights, data subjects may contact the Data Controller at: privacy@ama.it.

Data subjects also have the right to lodge a complaint with the competent Data protection Authority for the protection of personal data pursuant to Article 77 of the GDPR.