

PRIVACY

Information on the processing of personal data

Under the terms of articles 13 and 14 of EU General Data Protection Regulation 2016/679 of 26 April 2016 (hereafter referred to as the 'GDPR'), we provide the following information relative to the processing of personal data in the sphere of whistleblowing.

1. Who processes the personal data?

The controller of the personal data (hereafter also referred to as the 'Controller') is the A2A Group company which receives the whistleblowing report.

2. Who can be contacted?

For all queries related to the processing of personal data and the exercising of rights, contact the Data Protection Officer at the following e-mail address: dpo.privacy@a2a.it.

3. Who does this information cover?

For the purposes of whistleblowing, those involved, and whose confidentiality must be guaranteed, both in terms of identity and the contents of any communications, are the whistleblower, the subject of the whistleblowing report, any facilitator, other persons involved or mentioned in the report.¹

4. Why is personal data processed?

The purposes of the processing are:

- a) to receive, analyse and administer, through the appropriate channel of communication, reports – which may also be anonymous – relating to alleged irregularities and/or unlawful behaviour (i.e. whistleblowing reports) committed by persons who, for whatever reason, interact with the Controller, behaviour of which the whistleblower has become aware;
- b) to undertake all the further activities related to the processing of the whistleblowing report and necessary for the completion of investigation (e.g. the conducting of interviews, the gathering of all elements deemed useful for the purposes of the investigation, etc.) to be carried out by any competent body authorized to process any data involved;
- c) to enable response to any requests advanced by competent bodies and authorities.

5. What are the legal grounds for the processing?

For all of the aforementioned purposes, the juridical grounds which legitimize the processing are the compliance with a legal obligation deriving from the provisions of Legislative Decree no.231/2001, of Law 179/2017 and of Legislative Decree 24/2023 on the protection of persons reporting crimes, irregularities or violations of national regulations.

6. Which personal data is processed?

Whistleblowers may identify themselves or submit their report anonymously. In the case of an anonymous report, data relating to the whistleblower will not be processed unless required by law and/or authorized in advance by the whistleblower themselves.

For the purposes of the correct processing of the report and the completion of related activities, any data contained in the report and in any related documentation (that may refer to other identified or identifiable persons involved in the report) may be processed.

As examples, the following categories of personal data may be processed:

- personal information (e.g. name, surname, tax ID number, address, date and place of birth);
- contact data (e.g. telephone numbers, landline and/or mobile, e-mail address);
- professional data (e.g. seniority, company department, duties, type of relationship with A2A Group companies or other third parties, profession);

¹ Definitions

'Whistleblower': the person who submits the report or divulges information on violations of regulations within their working environment;

'Facilitator': a person who assists a whistleblower in the whistleblowing process, who operates in the same working context and whose help must remain confidential;

'Person involved': a person or legal entity mentioned in an internal or external report or in the publication as the subject to whom the violation or irregularity is attributed, or as a person in some way involved in the violation reported or put in the public domain.

- image and/or voice data;
- any information relating to the subject of the whistleblowing report or other persons involved who the whistleblower decides to share in the report in order to provide further detail;
- information which the subject of the report, or other persons involved, share with the Controller in the sphere of the processing of the report;
- other specific data (e.g. data concerning political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data serving to incontestably identify a person, data relating to the health or sexual life or sexual orientation of the person);
- legal data;
- other data relating to the whistleblowing report and which may or may not fall within the categories indicated above.

7. How is the data processed?

The processing is carried out by the personnel authorized to do so (members of the Whistleblowing Committee and assistance team and, if the whistleblowing report should concern violations of Legislative Decree 231/2001 or of organizational models of A2A Group companies, members of the Controller's Supervisory Body) and specifically trained for the processing of whistleblowing reports, who require knowledge of the information in the performance of their duties, with or without the support of electronic equipment, in accordance with the principles of lawfulness and correctness so as to safeguard at all times the confidentiality and rights of the parties involved in compliance with law. Reports, both anonymous and non-anonymous, may be sent by means of the dedicated communication channel using various formats, including audio and video recordings, in order to facilitate and optimize the reporting procedure. Furthermore, it is possible for the whistleblower to attach files and other documentation for the purpose of attesting to the validity of the report.

In order to safeguard confidentiality and guarantee anonymity, technical and organizational measures have been taken. These include, for the SAW platform, an encrypted connection which does not memorize the IP address of the user.

Moreover, following the sending of the message to the SAW platform, the whistleblower receives access data for the platform's Inbox so as to be able to continue communicating safely with authorized personnel.

Personal data which is clearly not of use for the purpose of processing a specific report, if unintentionally gathered, is deleted once its relevance has been excluded.

In accordance with Legislative Decree 24/2023, those involved can be asked for specific authorization in the following cases:

- the disclosure of the identity of the whistleblower to persons other than those authorized to receive such information or to act on the report;
- the use of a recorded telephone line or of another system of recorded voice messaging for the report, for the purpose of documentation by means of recording on a suitable storage or replay device, or by means of a complete transcription of the recording;
- a whistleblowing report made orally in the course of an interview with authorized personnel for the purpose of documenting the report on a suitable storage or replay device, or by means of written minutes of the interview.

Those involved may be asked for specific authorisation accompanied by specific communication setting out the motives for the disclosure of identity in the following cases:

- in the disciplinary procedure, if the objection to the report is fully or partly founded and where the disclosure of the identity of the whistleblower is indispensable for the defence of the subject of the disciplinary procedure;
- in proceedings initiated as a result of internal or external reports, when such disclosure is also indispensable for the defence of any person involved.

8. Who is the personal data communicated to?

The personal data of the whistleblower or of other persons involved can be made available to:

- IT companies nominated as Controllers;
- the parent company (A2A S.p.A.), which can process the data as Controller on behalf of other companies of the Group;
- public authorities and other bodies operating as Controllers in accordance with legal obligations (judicial authorities, Corte dei Conti, ANAC).

The data of those involved will not be made public (made available to unspecified persons).

9. Is the data sent to other countries?

Personal data will be processed within the European Economic Area (EEA). If it should be necessary, under exceptional circumstances, to transfer personal data outside the EEA, such transfer will be made on the basis of a decision of acceptability by the European Commission, if applicable, or in the presence of adequate guarantees required by the GDPR.

10. For how long is the data kept?

Reports and relative documentation will be stored for the time necessary for the processing of the report and, in any case, for no longer than five years from the date of the communication of the final findings of the whistleblowing report procedure.

Personal data, if already processed in the sphere of the ongoing working relationship with the employer, will be kept in accordance with the terms indicated in the general employee information to be found in the corporate intranet.

11. Which rights can be exercised?

Those involved have the right to ask the Controller for:

- confirmation that processing of their personal data is or is not under way and, if under way, that they can have access to it (art. 15 - right of access);
- correction of personal data that is incorrect or the completion of incomplete personal data (art. 16 - right of rectification);
- the deletion of the data if there is motivation as foreseen in the GDPR (art. 17 - right to erasure);
- for limitation of the processing when one of the cases foreseen by the GDPR exists (art. 18 - right to restrict processing);
- to receive the information provided to the data controller in a structured format, for normal use and readable using an automatic device, and to transmit such data to another data Controller (art. 19 - right to data portability).

Right to object (art. 21). If processing should be performed on the basis of the legitimate interest of the Controller, those involved are informed that, at any time, as of this moment, they may oppose this processing. In this case, the Controller will cease processing of the personal data involved, except in the case of legitimate motives in order to proceed in the processing or verification, exercise or defence of a right in a judiciary seat.

To exercise their rights, those involved can send a message to the e-mail address dpo.privacy@a2a.it or make a written request addressed to the Group company responsible for the processing.

Except in the case of other administrative or legal complaints or appeals, those involved have the right to ask the Privacy Authority to ensure protection of personal data should they deem that its processing violates the GDPR (art. 77).

Limitation of rights of those involved.

The rights as set out from article 15 to article 21 of the GDPR and listed above cannot be exercised by request made to the Controller under the terms of article 77 if the exercise of such rights effectively and concretely jeopardizes the confidentiality of the identity of the person reporting violations of which he or she has become aware as a result of his or her working relationship or duties performed.

In particular, those involved are informed that the exercise of such rights:

- will be possible in accordance with legal or normative provisions regulating the sector (Law 179/2017 and Legislative Decree 24/2023);
- may be delayed, limited or excluded with communication of motivation sent to the person involved without delay for the time and within the limits in which this constitutes a necessary and proportionate measure, taking into account the fundamental rights and legitimate interests of the person involved for the purpose of protecting the confidentiality of the whistleblower; in such cases, the rights of the person involved may also be exercised by the Privacy Authority in the forms as set out in article 160 of Legislative Decree 196/2003 (Privacy Code), in which case, the Privacy Authority will inform the person involved of the completion of all the checks necessary or of a re-examination, and also of the right of the person involved to submit a jurisdictional appeal.

12. From which source does personal data originate?

The personal data is voluntarily provided by the persons involved. Refusal to provide such data may make it impossible to correctly process the report or any objection to the report which may be made.

13. Is the data subjected to automated decision making?

The data will not be subjected to decisions based solely on automated processing, including profiling, which may have legal effects that concern or significantly affect the persons involved.

14. Cookies

Cookies are typically strings of text which websites or portals ('publishers', or 'first parties') visited by the user or other websites, portals or web servers ('third parties') position and memorize – directly, in the case of publishers, and indirectly, by means of the latter, in the case of 'third parties' – within a terminal device available to the user.

In the sphere of the SAW platform, use is made only of technical cookies strictly necessary to guarantee the correct and optimal functioning of the platform itself. For the purpose of the installation and use of these technical cookies, the consent of the user is not required.

The user may block, delete or deactivate individual cookies by modifying the browser settings. Most browsers, in fact, allow users to set rules for the activation and deactivation of all or some of the cookies sent.

Instructions on the deactivation of cookies in the main browsers are available at the following links:

- [Chrome](#)
- [Explorer](#)
- [Safari](#)
- [Firefox](#)
- [Opera](#)

Further information is available on the dedicated page of the website of the Privacy Authority (<https://www.garanteprivacy.it/temi/cookie>).