WHISTLEBLOWING POLICY

AEP Ticketing solutions S.r.l.

CONSTELLATION SOFTWARE GROUP

AEP Ticketing solutions S.r.l.

Via dei Colli, 240
50058 - Signa (Florence)
Italy

Tel. +39 055 8732606
Fax +39 055 8735926

info@aep-italia.it
www.aep-italia.it
www.aep-italia.it/gdpr.policy

Share capital € 118,000
i.v. Florence Trib. Reg. 38914
C.C.I.A.A. Florence 367217
C.F./P. VAT 03504280482
RAEE NO. IT08020000001381

Index

1. Introduction

At AEP Ticketing solutions S.r.l. (hereinafter also the "Company"), we want to foster a culture whereby those who work for us, or with us, feel comfortable raising any concerns about illegal or unethical practices, or behavior that is not in line with our ethical principles. In keeping with our culture, we offer a variety of channels through which concerns about illegal and/or fraudulent activities can be reported.

We encourage the reporting of any wrongdoing (including suspected wrongdoing) as soon as possible, using one of the channels indicated below in this procedure. We devote appropriate attention to each report, conducting all investigations as deemed appropriate, and always respect the confidentiality of the reporting person. You may report your concerns about something that has happened in the past, is happening currently, or that you believe will happen in the near future. Reporting parties, when in good faith, should not be afraid of retaliation, even if the report turns out to be unfounded. IN CASE OF DOUBT, ASK!

It should be noted that this procedure (hereinafter also "Policy") is not part of any employee's employment contract and may be changed/updated at any time by the Company.

Purpose: The purpose of this Policy is to dictate operational guidelines for the handling of reports sent or transmitted, even anonymously, concerning alleged workplace irregularities, offenses, or non-compliance with laws, regulations, rules of conduct or Company procedures (with particular reference to violations of the Code of Ethics) of which one has become aware. This procedure describes and regulates the process of reporting alleged irregularities, providing the reporter (so-called whistleblower) with clear operational guidelines regarding the subject, contents, recipients and methods of transmission of reports, as well as regarding the forms of protection envisaged by the Company in accordance with regulatory provisions.

All stages of the process in question, from the sending of the report to its receipt by the recipients, to the analysis and processing of the report, are governed by this Policy to ensure the confidentiality of the reporter and his or her safety from possible retaliatory and/or discriminatory actions resulting from the report.

This Policy, approved by the Company's Board of Directors on October 18, 2023 and implemented consistently with that adopted by the Constellation Software Group, is designed to operate in conjunction with the Company's Code of Conduct. In case of inconsistency between the Code of Conduct and this Policy, the latter shall take precedence.

What is Whistleblowing and what can be reported?

"Whistleblowing" refers to the reporting/disclosure of information that relates to wrongdoing (including alleged wrongdoing), risks or dangerous situations that may cause harm to the Company, as well as to customers, colleagues, citizens, and any other category of stakeholders.

This may include:

1) malfeasance in (i) financial services, products and markets; (ii) prevention of money laundering and terrorist financing; (iii) consumer protection; (iv) privacy and personal data protection; (v) network and information system security; (vi) environmental protection; and (vii) public procurement;

2) fraud to the detriment of the State or the European Union and other conduct that does not comply with applicable laws and/or procedures referable to the Company that may otherwise cause the Company economic and/or reputational damage.

By way of example, conduct subject to reporting may include:

- bribery, extortion, theft, improper offers of payment or improper entertainment to obtain unfair advantages;
- Unfair competition and antitrust laws;
- Harassment, sexual or physical abuse, or other unethical behavior;
- discrimination on the grounds of age, race, gender, sexual orientation, disability, religious belief, etc;
- Privacy and data protection violations;
- improper bookkeeping, financial integrity violations;
- unlawful activities that have not yet taken place but which the whistleblower reasonably believes may occur in the presence of concrete, precise and concordant evidence.

It is not necessary to have proof that such an act was committed; reasonable belief is sufficient. The reporter is not responsible for investigating the matter; It is the responsibility of the recipients of the report to ensure that an investigation takes place.

Who can file a report:

This procedure applies to all individuals - internal or external to the Company - who interact or have interacted on an ongoing basis with the activities of AEP Ticketing solutions S.r.l, including: Company personnel, including probationary workers, former employees, and candidates in personnel selections; self-employed workers, collaborators, freelancers, and consultants who work for the Company; volunteers and interns (paid and unpaid); shareholders; persons with administrative, management, control, supervisory, or representative functions at AEP Ticketing solutions S.r.l.; suppliers; and contractors.

The Report

Any communication regarding conduct in violation of the law or internal regulations that may occur or is about to occur or that in any other way falls within the definition of Whistleblowing must be sent immediately - even anonymously - as detailed below.

Reports must be made in good faith, be substantiated, and be based on precise and concordant evidence. To this end, it is expected that the reporter will proceed to:

- Accurately describe the fact being reported;
- Indicate the person(s) believed to be responsible for the violation(s), as well as any others involved and/or who may report on the fact or incur potential harm;
- describe the circumstances of time and place under which the reported event occurred, any measures taken to conceal the problem, and/or whether the problem was disclosed to anyone within the organization;
- describe the alleged violation, including the concrete manner in which the unlawful conduct was carried out, as well as the particular interests pursued by the unlawful conduct;
- attach all available supporting documentation, including photographs and/or any other descriptive files or materials intended to support the report;
- Provide all the elements useful for reconstructing the fact and ascertaining the merits of the report.

Reported violations must be those that are expressly prohibited by law and affect public interest or the Company's interest in integrity. They may not relate to disputes, claims or demands related to personal interests of the reporting person that pertain exclusively to his or her individual working relationships or inherent in his or her working relationships with hierarchically subordinate figures.

2. How to file a report

Reporting mode

Reports should be submitted through the channels provided for this purpose, namely:

- internal channel (of the Group)
- channel managed by ANAC
- public disclosure
- report to the judicial or accounting authority

The use of the internal channel is favored and should take priority; only upon the occurrence of one of the conditions set forth in Article 6 or 15 of Legislative Decree 24/2023, respectively, is it possible to make an external report to ANAC or a public disclosure.

Signaling channels

A report can be made by one of the following alternative methods:

- By e-mail to one of the dedicated addresses: whistleblowing@aep-italia.it; compliance@modaxo.com or whistleblower@csisoftware.com;
- By internal/ordinary mail to: AEP Ticketing solutions S.r.l., c.a. Human Resources (HR), Via dei Colli No. 240, 50058 Signa (FI);
- Through csisoftware.alertline.com, an external platform operated by a third-party operator, EthicsPoint, which also allows the reporter to contact a toll-free number applicable to each location and in the preferred language;
- By contacting the 24/7 hotline (800-715-059), with the possibility of leaving a voice message.

It is also possible to request a face-to-face meeting and interface - both verbally and in written form - with one's direct or area manager to make the report. In this case, with the consent of the reporter, the meeting will be minuted for the purposes of report processing.

In compliance with the requirements contained in Law No. 179 of 2017, all reporting channels indicated above protect the confidentiality of the reporter, ensuring that the person who intends to reveal his or her identity receives adequate protection and goes free from retaliatory and/or discriminatory acts. Notwithstanding, it is clarified that any report can be made anonymously, as long as the report is sufficiently substantiated and such as to allow for the appropriate investigations.

The reporter who is found to be involved in the reported violation should specify this, as he or she may receive different treatment than other responsible parties, consistent with applicable regulations.

No personal information should be included in the report beyond what is strictly necessary to analyze and follow up on it.

ANAC Channel

The competent authority for external reports is ANAC (www.anticorruzione.it), to which a report can be submitted only where one of the following conditions is met:

- If an internal reporting channel is not provided, is not active, or does not comply with legal requirements;
- The internal report did not give rise to a follow-up;
- There are reasonable grounds to believe that if an internal report were made, it would not be effectively followed up or could result in the risk of retaliation against the reporter;
- There is good reason to believe that the violation may constitute an imminent or obvious danger to public interest.

Public disclosure

Public disclosure is that mode of reporting that puts a report in the public domain through print, electronic media or, more generally, with all those of dissemination that allow to reach a large number of people (e.g., TV, Social Network...).

A whistleblower who makes a public disclosure benefits from the protection provided by the current whistleblowing regulations if, at the time of the disclosure, one of the following conditions is met:

- The reporting person has already made an internal and external report (or made exclusively an external report) and there has been no response within the stipulated time frame regarding the measures planned or taken to follow up on the reports;
- The reporting person has reasonable grounds to believe that the violation may pose an imminent or obvious danger to public interest;
- The reporting person has well-founded reason to believe that the external report may carry the risk of retaliation or may not be effectively followed up because of the specific circumstances of the case, such as those where evidence may be concealed or destroyed or where there is a well-founded fear that the reporting person may be colluding with or involved in the violation.

3. Recipients of internal reports and timing of feedback

The handling and verification of the merits of the circumstances represented in the report are entrusted to the Group's Legal Department (the "Legal Department"), which does so in accordance with the principles of impartiality and confidentiality, and any other individuals who may be consulted and/or have bearing with regard to the reported facts (including independent outside consultants, accountants and/or other specialists who may be appropriately engaged).

4. Management of internal reports

The Legal Department is entrusted with all activities related to the management, investigation/verification of reports submitted, as well as any measures deemed necessary.

Reports received are noted in a special register, maintained in accordance with the indicated principles of confidentiality.

The recipients of the reports receive them, examine them, and take all initiatives deemed necessary - including the preparation of minutes of any meetings concerning the investigative activities conducted independently and/or with the assistance of the corporate functions involved - to ascertain the merits (or otherwise) of the same. In carrying out the assessment activities, the recipients may involve other functions of the Company and/or appoint external consultants, if necessary, subject to the same confidentiality obligations and responsibilities to which the recipients of the report are subject.

In the case of a non-anonymous report, the reporter will receive confirmation of receipt within seven days.

Where they deem it necessary and/or appropriate for the purpose of ascertaining the merits of the report, the recipients of the report may:

- Contact the reporter (if not anonymous) and summon him or her for a personal and confidential interview in order to receive clarifications and/or additions to the information and documents provided;
- Interview any other individuals who can report on the reported facts;
- Carry out any other activities deemed appropriate for the purpose of investigating the report.

In case of a non-anonymous report, the Legal Department shall inform the reporter of the outcome of the investigation and any measures taken or in the process of being taken within three months from the date of notice of receipt (or, in the absence of such notice, within three months from the date of expiration of the seven-day period from the submission of the report).

In the event that, as a result of the investigations conducted, the report turns out to be well-founded (or at any rate appears to be so), the Legal Department shall promptly notify the competent parties of the reported unlawful conduct and/or violations, who will take appropriate measures in compliance with Company policies and current regulations.

5. Protection of the reporter from retaliatory and/or discriminatory acts

The whistleblower, as well as those who cooperated in the investigation/investigation of the report, may not be sanctioned, demoted, dismissed, transferred, or subjected to any other organizational measure having direct or indirect negative effects on working conditions determined by the report.

Retaliatory actions can take different forms, including:

- Threats;
- Disciplinary action (e.g., fine, suspension from work and pay, dismissal);
- Any action that prevents or restricts someone from speaking;
- Damage to a person's property, reputation, business or financial standing;
- Retrocession/demotion or denial of promotion;
- Intimidation, harassment, exclusion or humiliation.

They may also include "subtle" behaviors, such as:

- Hiding information that could help an employee fulfill his or her duties;
- Exclusion from social functions;
- Failure to assign a meaningful assignment;

- The use of language, whether verbal or body language, that is different compared to previous communications or communications with others.

Without prejudice to the right to compensation and any other applicable safeguards, anyone who believes that he or she has been retaliated against for reporting a matter or participating in an investigation, or believes that someone else is being retaliated against (even if he or she is outside the organization), is urged to report it immediately using the channels indicated in § 2. In addition, individuals who engage in retaliatory, discriminatory, or unfair conduct against the reporting person and others involved in the reporting may be subject to disciplinary proceedings, where applicable, including dismissal.

6. Safeguarding the confidentiality of the reporter

The Legal Department, as well as the other parties that may be involved in the process, is committed to ensuring the utmost confidentiality of the reporter, protecting his or her identity, from the moment the report is taken, also to avoid the risk of retaliation and/or discrimination against the person making the report. In fact, except as provided for by law (e.g., criminal, tax and/or administrative investigations, inspections by supervisory authorities), the identity of the reporter cannot be revealed without the written consent of the person concerned.

However, in the event that the reports are reported to the Authorities, the obligation to keep confidential the identity of the persons involved or mentioned in the report may be waived in the manner and under the conditions provided by applicable law. Should it be obligatory, indispensable, or legitimate under applicable law to disclose the identity of the reporting person to the Authority, the reporting person will be informed by the Company of the reasons for such disclosure.

All communication with the reporter takes place through the same channel originally used by the reporter for reporting. In the information regarding the processing of personal data (given to the reporter at the time of the report, including via telematic platform), the reporter is informed of the possibility for which the report could be lawfully forwarded to the competent persons or authorities.

7. Responsibility of the reporter

It is the responsibility of the reporter - even anonymous ones - to make reports in good faith and in line with the stated spirit of this Policy. Without prejudice to the criminal and disciplinary relevance for slanderous or defamatory reports, reports that are manifestly unfounded, opportunistic and/or made for the sole purpose of harming the reported person or subjects otherwise affected by the report will not be taken into consideration and will be subject to sanctions and/or disciplinary procedures and/or actions before the competent Judicial Authority.

8. Rights of the person being reported

During the activity of verification and ascertainment of potential irregularities, the subject(s) of the report (so-called reported) may be involved or notified of such activity but in no case will a sanctioning procedure be initiated against them on the basis of the mere report (that is, in the absence of concrete evidence with respect to the content of the report). This may be done on the basis of concrete evidence found and ascertained on the basis of the report itself, and always in compliance with current regulations.

9. Privacy

Pursuant to the Regulation (EU) 2016/679 (hereinafter, "GDPR") and the current national legislation on the protection of personal data (hereinafter, together with the GDPR, the "Privacy Legislation"), AEP Ticketing solutions S.r.l., based in 50058 Signa (FI), Via dei Colli no. 240 (hereinafter also the "Data Controller"), as the Data Controller, is required to provide the information regarding the use of personal data collected as part of the reports and related investigative activities.

The Data Controller may process personal data collected in the context of channels established in compliance with applicable regulations, to enable the reporting of violations of national and European regulations that harm the public interest or the integrity of the Company (so-called whistleblowing), as well as for the handling of such reports.

This disclosure applies to individuals who report such violations, reported individuals named as alleged perpetrators, individuals implicated in the violations, and individuals aware of the facts or otherwise mentioned in the report.

Data. The handling of reports involves processing both the personal data of the reporter (in case the reporter is named) and those of the reported person(s).

The identity of the whistleblower should never be disclosed to the person who is the subject of the report, except in cases provided for by law. This is to avoid retaliation, threats, violence, etc., as well as to protect the confidentiality of the whistleblower. That said, if there is a substantial risk that the disclosure of the relevant information may jeopardize the ability to effectively verify the basis of the report or to obtain the necessary evidence, the reported person may not be informed about the recording of his or her data, for as long as necessary to ensure the proper handling of the investigation and in any case in accordance with the provisions of the applicable national collective agreement. Under no circumstances may the reported person use his or her right of access to obtain information about the identity of the whistleblower, unless the whistleblower has made a complaint in bad faith.

Processing may cover, in addition to common personal data, indicative data; contact data; data relating to alleged reported conduct attributed to the reported person, in which the data subject may be involved or of which he or she may have knowledge; images and other documentation attached to the reports; special categories of personal data that may be contained in the reports; contents of communications exchanged between the reporter and the persons handling the reports; as well as sensitive personal data, i.e., those revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; or trade union membership; data relating to a person's health or sex life or sexual orientation. Sensitive data correspond to data belonging to the "special categories" indicated in Art. 9 of Reg. (EU) 679/2016 (known as GDPR).

Such data will only be processed where strictly necessary for the handling of the report, in accordance with the principles of proportionality and necessity.

Purpose and manner of data processing. The processing will take place for the purpose of managing, processing, investigating, and resolving the report, as well as to establish any disciplinary measures or otherwise to take measures appropriate to the specific case. The provision of a useful tool for the management of reports meets precise requirements for the Company's internal control and monitoring of business risks, specifically dictated by law.

Data are processed using manual, computerized and telematic tools with logic strictly related to the stated purposes and, in any case, in such a way as to ensure the security and confidentiality of the data, in accordance with the provisions of the relevant legislation in force.

Legal basis. Processing activities are carried out on the basis of a legal obligation to which the Data Controller is subject (Art. 6(1)(c) GDPR), pursuant to the applicable whistleblowing legislation. If, as part of a whistleblowing, special categories of data are provided, the Data Controller will process them pursuant to the following exceptions provided for in Article 9 GDPR consisting of: (i) the need to fulfill the obligations and exercise the specific rights of the Data Controller or the data subject in the field of labor and social security law and social protection (Art. 9(2)(b) GDPR). (b) GDPR); and (ii) in the need to ascertain, exercise or defend a right in judicial proceedings or whenever judicial authorities exercise their jurisdictional functions (Art. 9(2)(f) GDPR) with regard to the processing of personal data necessary in litigation or pre-litigation, to assert or defend a right, including the right of the Data Controller or a third party, in judicial proceedings, as well as in administrative proceedings or arbitration and conciliation.

Provision of data. The provision of personal data on the reported person for the purposes related to the management of reports is strictly necessary. Failure to provide the data of the person who is the subject of the report (so-called reported person) will result in the impossibility of fulfilling the verification activity described above. On the other hand, the provision of the reporter's personal data is optional.

Communication and dissemination of data. The data contained in the reports may be communicated and/or disseminated only to those specifically authorized by the Company, as well as to the Judicial Authority, in order to investigate and carry out the investigative activity of the report and possibly activate the judicial and/or disciplinary protection related to the report. In any case, the identity of the reporter, and any other information from which it can be inferred, may be disclosed to parties other than employees or external parties authorized to handle the report or investigation on behalf of the Data Controller, only with the authorization of the reporter or when obligatory or legitimate under applicable regulations. In exceptional cases, where disclosure of identity is indispensable for the defense of the reported person (within the scope of disciplinary proceedings) or the person involved (within the scope of internal procedures), the reporting person will be informed in writing by the Company of the reasons for such disclosure. The protection of confidentiality is also guaranteed to the other persons concerned, until the conclusion of the proceedings initiated on account of the report and in compliance with the same guarantees provided in favor of the reporter. However, in the event that the reports are reported to the competent authorities, the obligation of confidentiality of the identity of the persons involved or mentioned in the report may be waived in the manner and under the conditions provided by the applicable regulations.

The data subject to the report may be communicated, if necessary and in accordance with the principles of proportionality and non-excessiveness, to auditing companies and/or consultants of AEP Ticketing solutions S.r.l. or related companies involved. This is subject to legal obligations and the protection of the rights of the data controller or persons (natural or legal) however involved and/or related to the report.

To the extent strictly necessary and, in any case, subject to appropriate safeguards, data may be processed by companies that provide the Data Controller with information systems and/or companies that are involved in their maintenance and security.

Transfer of data abroad. Personal data may be transferred outside the national territory (including outside the European Economic Area) for the purpose of managing and/or processing the report. In any case, such transfer will take place in compliance with applicable regulations by assuming the appropriate safeguards.

Data Retention. In accordance with the principles of proportionality and necessity, personal data will be kept in a form that allows the identification of the data subjects for the time necessary to

process the report and, in any case, no longer than five years from the date of the communication to the reporter of the final outcome of the reporting procedure. This is without prejudice to any specific regulatory obligations or the Data Controller's supervening need to act or defend itself in court, which make it necessary to process and store data for additional periods of time.

Rights of the data subject. At any time, the data subject may obtain confirmation of the existence or non-existence of his or her data and to know its content and origin, verify its accuracy or request that it be supplemented or updated, or corrected (Articles 15 and 16 of the GDPR). In addition, he/she has the right to request the deletion, restriction of processing, revocation of consent, and portability of data as well as to lodge a complaint with the supervisory authority and to object in any case, for legitimate reasons, to their processing (Art. 17 et seq. of the GDPR).

The data subject may also request the full list of data recipients at any time.

These rights may be exercised by written notice to be sent to: alessandro.agostini@macroazienda.it or, by regular mail, to the address of the Company (AEP Ticketing solutions S.r.l. Via dei Colli no. 240, 50018 Signa (FI)) to the attention of the Data Protection Officer (DPO).

The Data Controller, including through designated facilities, will take up the request and provide the data subject, without undue delay, with information regarding the action taken regarding the request. The data subject is advised, however, that the exercise of his or her rights may be restricted or excluded if actual and concrete prejudice to the confidentiality of the identity of the reporter may result from the exercise of such rights.

For information or clarification of rights, or the processing of personal data, the data subject may contact the same contact details.

Data Controller. The Data Controller is AEP Ticketing solutions S.r.l. with headquarters in 50018 Signa (FI), Via dei Colli no. 240.

AEP Ticketing solutions S.r.l. has designated the Managing Director as the Data Protection Officer. The Managing Director can be contacted at the following address: gdpr@aep-italia.it

10. Procedure dissemination and training

This Policy - published on the Company website - will be communicated, illustrated and disseminated, in all its parts, to all Managers and staff (collaborator and/or employee) of AEP Ticketing solutions S.r.l, as well as to all those third parties interested in compliance with the requirements contained therein.

Training to staff will take place through computer-based modes.

11. Final clauses

The Constellation Software Group Legal Department is responsible for the implementation of this misconduct reporting policy and will be responsible for monitoring its implementation, systematically checking its adequacy and effectiveness, and responding to any requests for clarification of its contents.