Policy regarding the reporting of irregularities noted within Autonom Services S.A. (Whistleblowing Policy)

This Policy describes the way in which Autonom Services S.A. offers support so that you can point out the irregularities noted, which have an impact on the company, express your concerns in a safe manner, know whom to contact, the specific way of reporting and the rights you have as a whistleblower, as well as the safety measures applicable to you if you report an irregularity.

LAST UPDATE: August 2022

Contents

Chapter I. Introduction. Purpose of the Policy. Legal benchmarks

Autonom Services S.A. undertakes to comply with the highest standards of transparency, ethics, probity and responsibility, which represent genuine values of the company. These elements are crucial for maintaining the reputation of the company and its present success.

A key aspect of enforcing these values is a mechanism allowing the company's staff and collaborators to voice their concerns related to the irregularities noted within the working environment, which have already been committed or are likely to occur, in a responsible and effective manner. The basis for any employment or collaboration relationship is the ability of every employee or collaborator to be faithful to their employer/partner and not disclose their confidential information in an uncontrolled manner. However, if an individual discovers information that they consider to be likely to constitute a breach of law, of the rules of conduct or the provisions of the internal rules, of the internal policies or procedures or of the ethical norms promoted within Autonom Services S.A., this information should be revealed internally, without fear of retaliation.

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 offers legal protection to persons who report such conduct, which not only disregards societal values, but also goes against legal provisions – protection against dismissal, enforcement of disciplinary penalties or termination of contractual relations by Autonom Services S.A. as a result of revealing the breaches to the persons responsible for the resolution of the reported cases. Autonom Services S.A. approved the provisions of this Policy in order to ensure that no staff member or collaborator will be disadvantaged in the context of reporting inappropriate conduct, actions or omissions, as well as in order to offer whistleblowers an effective reporting procedure.

The aim of this Policy is to provide whistleblowers with an efficient means of reporting information on breaches which was acquired in a work-related context and is reasonably believed to be true at the time of reporting. This Policy is not intended to be used in order to question the financial or business decisions taken by Autonom Services S.A., nor should it be used arbitrarily or as a vexatious tool for the company's staff.

People who work for a private organization, regardless of the form of collaboration, or who are in contact with such an organization in the context of their work-related activities are often the first to find out about acts that have a significant impact on the organization. By reporting such breaches, they act as whistleblowers and thus play an essential role in exposing and preventing such acts. However, fear of retaliation often discourages potential whistleblowers from reporting their concerns or suspicions. For that reason, the company has drawn up this Whistleblowing Policy, which is an important element in the detection of corrupt or unlawful conduct or of other types or undesirable conduct which go against societal

interests. In this regard, the company encourages its staff to initiate the reporting process in situations where there is any suspicion or knowledge of irregularities or breaches of the legal rules and the internal provisions of Autonom Services S.A., while committing itself to guarantee the protection of whistleblowers in cases where it is found that they have reasonable grounds to believe that the information on the breaches reported is true at the time of reporting and that the information reported falls within the scope of this Policy.

Legal benchmarks taken into account while drawing up this Whistleblowing Policy

- 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;
- REGULATION (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- Codul Muncii (Labor Code) – Law no. 53/2003 – republished;
- Legea nr. 21 din 10 aprilie 1996 a concurenței (Competition Law no. 21 of 10 April 1996);
- Noul Cod Civil (the new Civil Code);
- Legea nr. 71/2011 pentru punerea în aplicare a Legii nr. 287/2009 privind Codul Civil (Law no. 71/2011 for the implementation of Law no. 287/2009 on the Civil Code);
- Legea privind protecția avertizorilor în interes public (PL-x nr. 219/2022, L nr. 175/2022) [Law on the protection of whistleblowers (PL-x no. 219/2022, L no. 175/2022)];
- Cererea de reexaminare asupra Legii privind protecția avertizorilor în interes public (Request for the review of the Law on the protection of whistleblowers), referred to the Parliament for review on 28 July 2022 by the President of Romania, Klaus Iohannis.

Chapter II. Definitions

a) **"breaches"** are acts consisting of an action or a lack of action in violation of the legal provisions, acts that disregard the provisions of the internal rules and that represent instances of misconduct, offences or crimes, or that defeat the object or the purpose of the law, acts that disregard the internal policies and procedures applicable within Autonom Services S.A., actions or omissions that violate ethical norms, the rules of conduct or the values of the company;

b) "**information on breaches"** means information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the organization in which the reporting person works or has worked or in another organization with which the reporting person is or was in contact through his or her work, and about attempts to conceal such breaches;

c) "**report"** means the oral or written communication of information on breaches within the company. Internal reporting is carried out using the means made available by Autonom Services S.A. for reporting breaches, as detailed below. These constitute the internal reporting channels;
d) "**public disclosure**" means making available in any way, in the public domain, the information related to breaches;
e) "**whistleblower**" means the natural person who reports or publicly discloses information on breaches of law, acquired in a work-related context;
f) "**facilitator**" means a natural person who assists a reporting person in the reporting process in a work-related context, and whose assistance should be confidential;
g) "**work-related context**" means current or past work activities of any kind, whether paid or unpaid, carried out within the company, through which persons could acquire information on breaches of law and they could suffer retaliation if they reported such information;
h) "**employee**" means the natural person who is in an employment or service relationship pursuant to general or special legal provisions and performs work in exchange for remuneration;
i) "**collaborator**" means the natural person who is in a contractual relationship with Autonom Services S.A., regardless of the contractual form of collaboration or the payment of a remuneration.
j) "**person concerned by the report**" means the natural or legal person who is referred to in the report or public disclosure as a person to whom the breach of law is attributed or with whom that person is associated;
k) "**retaliation**" means any direct or indirect act or omission which occurs in a work-related context, is prompted by reporting or by public disclosure, and which causes or may cause detriment to the whistleblower;
l) "**follow-up**" means any action taken by the recipient of a report or by the competent authority for the resolution of the report and, where relevant, to address the reported breach;
m) "**informing**" means the delivery of information on the follow-up and on the reasons for such follow-up to the whistleblower;
n) "**competent authority for receiving reports of breaches of law**" means:
   i. public authorities and institutions which, in accordance with special legal provisions, receive and resolve reports of breaches of law in their area of competence;
   ii. the National Integrity Agency, hereinafter referred to as the Agency;
   iii. other public authorities and institutions to which the Agency submits reports for competent resolution.
o) "**designated person/Team**" means the person/team responsible for receiving, recording, examining, taking follow-up action and resolving reported cases, who shall act impartially and shall be independent in the exercise of the duties mentioned. Within Autonom Services S.A., the designated Team is made up of staff from the Human Resources Department, which signed a confidentiality agreement with the company, mainly covering the identity of the whistleblowers

in cases where they do not choose to remain anonymous, as well as the information of which they become aware while performing their duties.

p) "**feedback**" means the provision, by the designated Team, of information on the action envisaged or taken as follow-up and on the grounds for such follow-up to the reporting person;

q) "**management of the company**" means the Manager/Managing Director of Autonom Services S.A. or any other persons in managerial positions that the Manager or the Managing Director has mandated for this purpose;

r) "**direct discrimination**" means deeds and acts of exclusion, differentiation, restriction or preference, based on a person's gender, sexual orientation, genetic features, age, nationality, race, color, ethnicity, religion, political beliefs, social origin, disability, family situation or responsibilities, trade union membership or activity, which have the purpose or effect of denying, restricting or nullifying the recognition, use or exercise of the rights provided for by the labor legislation;

s) "**indirect discrimination**" means deeds and acts that appear to be based on grounds other than a person's gender, sexual orientation, genetic features, age, nationality, race, color, ethnicity, religion, political beliefs, social origin, disability, family situation or responsibilities, trade union membership or activity, but which produce the effects of direct discrimination;

t) "**harassment**" means a situation in which any form of unwanted conduct occurs in relation to a person's gender, sexual orientation, genetic features, age, nationality, race, color, ethnicity, religion, political beliefs, social origin, disability, family situation or responsibilities, trade union membership or activity, with the purpose or effect of violating the dignity of the person concerned and creating an intimidating, hostile, degrading, humiliating or offensive environment;

u) "**sexual harassment**" means a situation in which any form of unwanted verbal, non-verbal or physical conduct of a sexual nature occurs, with the purpose or effect of violating the dignity of a person and, in particular, of creating an intimidating, hostile, degrading, humiliating or offensive environment;

v) "**gender discrimination**" means instances of direct and indirect discrimination, consisting of any form of unwanted conduct defined as harassment or sexual harassment displayed by one person towards another person in the workplace or in any other place where they perform their work-related activities, with the purpose or effect of:

   i. creating an intimidating, hostile or discouraging environment in the workplace for the victim;
   ii. negatively influencing the situation of the employee in terms of professional promotion, remuneration or income of any kind, or access to training and professional development, if the employee refuses to accept some form of unwanted conduct of a sexual nature;

w) "**multiple discrimination**" means any act of discrimination based on two or more discriminatory grounds;

x) "**personal data**" means any information relating to an identified or identifiable natural person ("**data subject"**). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data,

an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

y) "**processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

z) "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Chapter III. Principles

The principles governing the protection of reports of breaches and underpinning this Policy are the following:

a) **The principle of lawfulness**, according to which Autonom Services S.A. has an obligation to respect fundamental rights and freedoms by ensuring full respect for, inter alia, freedom of expression and information, the right to the protection of personal data, the freedom to conduct a business, the right to a high level of consumer protection, the right to a high level of human health protection, the right to a high level of environmental protection, the right to an effective remedy and the right of defense;

b) **The principle of responsibility,** according to which the whistleblower has an obligation to present data or information related to the reported acts;

c) **The principle of impartiality**, according to which the examination and the resolution of the reported cases are carried out in an objective manner, regardless of the convictions and interests of the persons responsible for their resolution;

d) **The principle of good administration**, according to which the company has a duty to operate in its own best interest, with a high degree of professionalism, in an efficient manner and with an effective use of resources;

e) **The principle of balance**, according to which no person may take advantage of the provisions of this Policy to reduce their penalty for a more serious offence that is unrelated to the reported case.

Chapter IV. Scope of the Whistleblowing Policy

Personal scope

This Procedure applies to whistleblowers, as previously defined, who acquired information on breaches, in the sense previously described, in a work-related context. The following persons fall within this category:

a) employees;
b) self-employed persons within the meaning of Article 49 of the Treaty on the Functioning of the European Union;
c) shareholders and members of the company's administrative, management or supervisory body, including non-executive members of the Board of Directors, as well as paid or unpaid volunteers and trainees;
d) any person working under the supervision and direction of Autonom Services S.A., on the basis of a contract, the company's subcontractors and suppliers;
e) whistleblowers who report information on breaches acquired in the context of an employment relationship that is ongoing, that has since ended or that has not yet begun, if the information on the breaches was acquired during the recruitment process or during other pre-contractual negotiations.

This Policy also applies to:

a) facilitators;
b) third parties linked to the whistleblowers who might suffer retaliation in a work-related context, such as colleagues or relatives of the whistleblowers; and
c) legal entities that the whistleblowers own or work for, or that are linked to the whistleblowers in other ways in a work-related context.

In addition, the Whistleblowing Policy applies to persons who submit reports, including in anonymous form, through the online reporting channel provided by the company, concerning information on breaches acquired during the recruitment process or during other pre-contractual negotiations, or in cases where the employment or service relationship is ongoing or has ended.

Cases where this Policy is not applicable

This Policy is not applicable in the cases described below. If it is established that the information was disclosed in one of the following contexts, the whistleblower will not be granted the rights mentioned in this document:

a) reporting of information already in the public domain (e.g. newspaper articles, information made public, rumors which are unsubstantiated or which have been heard, but are unverified, trivial findings, gossip or information unrelated to the performance of the whistleblower's duties;

b) disagreements over the content of company policies or over the rules or obligations imposed on staff members or collaborators, questions about one's personal performance or about the performance of another colleague/collaborator, and any other issues related to the human resources of Autonom Services S.A. and which are strictly of personal interest for a whistleblower;
c) breaches of public procurement rules or national defense and security rules.

Chapter V. Reporting procedure Key elements of a legal reporting process

Autonom Services S.A. has deployed an online reporting channel, which can be accessed by anyone interested via the following link: https://whistleblower.autonomservices.ro.

This reporting channel is designed, deployed and managed in a secure manner, so as to protect the confidentiality of the identity of the person submitting the report and the identity of any third party mentioned in the report, as well as the identity of the data subject, and to prevent access by unauthorized members of staff.

Thus, any person to whom this Policy applies and who becomes aware of acts that are likely to disregard legal or ethical provisions or provisions included in the internal procedures and policies or in the internal rules applicable at company level has access to an effective tool for reporting such acts.

What should we report?

Whistleblowers are encouraged to report breaches which have already occurred or are likely to occur within Autonom Services S.A., about which they acquired information in a work-related context and which concern:

a) provisions of the law, regardless of its nature (criminal, civil, or minor offences, breaches of labor law or environmental law, anti-competitive practices, actions or omissions that affect the safety and compliance of products, services, financial products and financial markets, as well as actions in the fields of prevention of money laundering and terrorist financing, public health, consumer protection, protection of private life and personal data and the security of networks and information systems, etc.);
b) the provisions of the internal rules applicable at company level;
c) the provisions contained in the policies and procedures applicable within Autonom Services S.A., which may refer to aspects including, but not limited to: workplace conduct, working conditions or workplace practices, etc.;
d) acts of harassment, regardless of its nature, acts of discrimination or aggressions in the working environment;
e) workplace conflicts which have already occurred or are likely to occur.

When should we report irregularities?

The staff of Autonom Services S.A. or the collaborators of this company are encouraged to report irregularities when:

a) they notice breaches, as defined in this Policy;
b) they note that a number of breaches are likely to be committed within Autonom Services S.A;
c) there are reasonable grounds to believe that the information on breaches reported is true at the time of reporting and that this information falls within the scope of the Policy.

Which elements must be included in the report?

The report shall include at least the following elements:

a) the work-related context in which the information was acquired;
b) the person concerned, if known;
c) the description of the act which is likely to constitute a breach occurring within Autonom S.A.;
d) the provisions of the law/internal rules and policies considered to have been breached;
e) the evidence supporting the report, including documents (if the whistleblower does not have access to the evidence, their type or location shall be indicated);
f) the date when the breach was committed or noted;
g) the place where the breach was noted;
h) the measures to be taken for the purpose of punishing the breach/preventing its occurrence;
i) the contact details, name and surname of the whistleblower, but only if the whistleblower decides to reveal this data, as this letter does not represent a mandatory element of the report.

How should we report irregularities?

Autonom Services S.A. has offered its staff and collaborators an efficient and secure tool, which complies with legal requirements relating to reporting. Thus, reporting can be done online, through the software that can be accessed by the staff on the company's website.

1. A report can be submitted via the following link: www.whistleblower.autonomservices.ro
2. Before submitting a report, it is recommended to refer to this Whistleblowing Policy, available at the bottom of the web page and at the level of the welcome message. It is also recommended to read the content of the Information Note on GDPR, attached to this Policy, which explains the processing the data involved in the processing activity, which can belong to both the whistleblowers (if they choose to reveal their identity) and the persons concerned.

3. The whistleblower will access the REPORT section on the home page. They will make sure that the previously mentioned requirements related to the content of the report are observed. The following types of information will be included: the description of the irregularity/breach, how it happened, what is being breached (internal rules, employees' rights, legal provisions, internal procedures and policies, etc.), the place where the breach was committed, the period, time and date of the breach, as well as whether or not it is a repeated breach, evidence or documents proving the breach, in any format, the measures to be taken for the purpose of punishing the breach or preventing its occurrence, as well as the identification details of the whistleblower, but only to the extent in which they decide to reveal their identity.
4. The reporting form will be filled out by completing the following fields:
   a. Anonymity checkbox: if the whistleblower wishes their identity not to be revealed, they will check the *Anonymous* box. If the whistleblower chooses to remain anonymous, their IP address cannot be tracked and will be deleted each time a report/additional information is submitted (their IP address is never stored on the servers of Autonom Services S.A.). Therefore, any metadata used for identification purposes, from most types of files shared, will be removed. In order not to prejudice confidentiality, each reporting case will receive a unique, randomly generated code. This code will have to be memorized by the whistleblower in order to access the status of the report or to submit possible additional information/responses, etc.
   b. *Subject*: The subject of the report will be mentioned briefly.
   c. *E-mail address* (this is an optional field, which will be completed only if the whistleblower decides to reveal their identity). The professional e-mail address will be provided.
   d. *Documents*: in this field, the whistleblower will upload the evidence (document, text, audio, video, mp3, mp4) supporting the report. If the whistleblower does not have access to the evidence, they will specify in the Suggestion or complaint box what the evidence is and, if known, where it can be obtained.
   e. *Suggestion or complaint*: In this field, the whistleblower will describe the breach and indicate the measures deemed necessary to prevent the occurrence of the breach or to punish the irregularity, depending on its seriousness.
   f. By clicking on the *SEND* button, the report will be directed to the designated Team.
   g. To check the status of the report or the response provided, the whistleblower will access the *CHECK* section and enter the randomly generated code, which was assigned to the report and previously saved by the whistleblower.
   h. Log in
5. The team designated for receiving reports and resolving the reported cases has the obligation not to reveal the identity of the whistleblower, nor the information that would allow their direct or indirect identification, unless the whistleblower has expressly consented to it. However, the identity of the whistleblower and any other information previously referred to may be disclosed only if required by law, subject to the conditions and limits laid down therein. In the latter case, the

whistleblower is informed in advance, in writing, via the online platform, of the disclosure of their identity and the reasons behind the disclosure of the confidential data in question. This is not required in cases where informing the whistleblower would jeopardize investigations or judicial proceedings. The information contained in the reports that constitutes trade secrets may not be used or disclosed for purposes other than those necessary for the resolution of the reported case.

6. The duty of confidentiality does not apply if:
   i. the whistleblower intentionally revealed their identity in the context of public disclosure.
7. The duty of confidentiality shall still be observed if the report accidentally reaches another person working for Autonom Services S.A., who is not a member of the designated Team. In that case, the report shall immediately be forwarded to the designated person.
8. The designated Team shall send the whistleblower a confirmation of the receipt of the report within 7 calendar days of receipt. To view this confirmation, the whistleblower will access the *CHECK* section of the platform.
9. The whistleblower shall be informed of the status of the follow-up no later than 3 months after the date when the receipt of the report was confirmed or, if the receipt of the report has not been confirmed, after the expiry of the 7 calendar days period previously mentioned, and thereafter, whenever there are developments in the follow-up process, unless informing the whistleblower could jeopardize the follow-up.
10. The designated Team shall inform the management of Autonom Services S.A. on how the reported case will be resolved.
11. Moreover, the designated Team shall inform the whistleblower on how the reported case will be resolved.
12. Communication between the whistleblower and the designated Team shall be carried out exclusively through the internal reporting channel previously mentioned.

Chapter VI. Closure of reported cases

Reported cases are closed if they do not contain the mandatory elements laid down in this Policy, other than the identification details of the whistleblower (name, surname, e-mail address, etc.), and the designated Team has requested the completion of the report, but the whistleblower did not fulfil this obligation within 15 days.

If a person submits several reports on the same subject, the reports shall be linked and the whistleblower shall only receive one information notice from the designated Team. After sending the information notice, if the designated Team receives a new report with the same subject, without providing additional information justifying a different follow-up, the new one shall be closed.

The designated Team may decide to close the procedure if, after examining the report, it is found that the reported act represents a clearly minor breach and that the only follow-up necessary is the closure of the procedure.

However, the duties to maintain confidentiality, to inform the whistleblower of the measures taken and not to prejudice any other obligations or applicable procedures to remedy the reported breach remain.

Any closure decision shall be communicated to the whistleblower via the online platform, indicating the legal basis.

Chapter VII. Resolution of reported cases

Every report submitted shall be treated seriously by the designated Team, so as to thoroughly analyze all issues raised in order to determine the need for follow-up and its nature.

Reports submitted via the form available on the online platform are managed in a secure manner, in order to protect the confidentiality of the identity of the whistleblower or of any third party and to prevent unauthorized access by the staff members of Autonom Services S.A. to the reported data and information.

The reception, registration, examination and resolution of reported cases fall within the competence of the Human Resources Department. For this purpose, a responsible Team shall be appointed, i.e. a committee shall be set up, consisting of members of the HR Department, depending on the complexity of the report, who shall remain independent and impartial.

The designated Team shall proceed with the confirmation of the receipt of the report within 7 days of receipt via the platform.

The designated Team shall review without delay the report impartially, objectively and by taking into account all the elements and circumstances, in order to determine whether it contains sufficient evidence to support the information on the breaches mentioned.

Any investigation shall be conducted swiftly and efficiently, and its duration may vary depending on the case. The principles of fairness of investigation, impartiality and equality of all parties involved shall be observed.

Not every report will lead to follow-up, only those that are substantiated and contain sufficient information about the reported breach, i.e. sufficient evidence to support the issues described in the report.

After the completion of the analysis of the reported case, the designated Team shall draw up a report, which shall be subject to confidentiality and shall contain conclusions and proposals for measures to be taken, if appropriate. The report will be submitted to the company's management.

Autonom Services S.A. shall send a response to the whistleblower regarding the reported case within a reasonable period of time and no later than 3 months after confirmation of receipt. If no confirmation has been sent, the response shall be delivered no later than 3 months after the expiry of the 7-day period following the reporting. The whistleblower shall also receive information on the progress of the investigation, unless this jeopardizes the investigation.

The responses, i.e. the information related to the investigation, if it needs to be communicated, can be accessed by the whistleblower in the *CHECK* section, by entering the reference code initially generated.

NOTE: Autonom Services S.A. reserves the right not to provide the whistleblower with confidential information, the disclosure of which is forbidden according to the legislation in force and the internal policy of the Company.

If the report is justified, Autonom Services S.A. may proceed with disciplinary measures proportionate to the seriousness of the breach, according to the internal procedure, respectively with informing the competent bodies (criminal, civil, etc.) in order for legal procedures to be carried out, as appropriate.

CHAPTER VIII. Advice, information and assistance provided to whistleblowers

Advice and information on protection measures, rights, procedures and remedies applicable to whistleblowers are provided by the National Integrity Agency (the *Agency*).

The Agency offers assistance to whistleblowers in relation to their protection against retaliation before any authority.

CHAPTER IX. Protection of the identity of the data subject and third parties

Confidentiality of identity is a key factor for Autonom Services S.A. Therefore, the protection of the identity of the data subject and the third parties referred to in the report is ensured by keeping it confidential.

The Team designated for resolving the reported case has the duty not to disclose the identity of the data subject or third party or any information that would directly or indirectly lead to their identification. The designated person is not bound by this obligation if the data subject or third parties have expressly consented to the disclosure of their identity, as previously stated.

However, the identity and identifying information may be disclosed if required by law, subject to specific conditions and limitations. In this situation, unless it jeopardizes the investigation or legal proceedings, the person concerned shall be informed in advance, in writing, of the disclosure of their identity and the reasons behind it.

The identity of the data subject is protected as long as the follow-up of the report or public disclosure is ongoing, unless, following the resolution of the report or disclosure, it is determined that the data subject is not guilty of the breaches of law that were the subject of the report or disclosure.

Data subjects have the right of defense, including the right to be heard and the right of access to their own file.

CHAPTER X. Obligations of whistleblowers

Whistleblowers have the following obligations:

1. to submit data or information on the acts reported;
2. not to make a report based on facts they know are not true;
3. to include in the report at least the information previously referred to, with the exception of identification details;
4. to submit the additional information requested by the designated Team within 15 days from the moment when the request was communicated, failing which the case reported shall be closed;
5. to have reasonable grounds to believe that the information on breaches reported was true at the time of reporting and that this information was within the scope of the reporting process;
6. in order to qualify for protection, the whistleblower must have reported either internally or externally or must have made a public disclosure, and the information on the breaches must have been acquired in a work-related context.

NOTE: Whistleblowers may be held liable under general provisions of law only for acts or omissions which are not related to reporting or public disclosure or which are not necessary for revealing a breach.

CHAPTER XI. Record keeping of the reports

The reports shall be recorded in a register, which must be kept by Autonom Services S.A. in an electronic format and which contains the reference code assigned to the whistleblower, the subject of the report and the resolution method.

Autonom Services S.A. keeps records of every report received, in compliance with confidentiality requirements, for a period of 5 years. After this period, the reports shall be destroyed, regardless of the form in which they are kept.

Where, for any reason, a telephone line or another voice messaging system is used for reporting, the designated Team is required to document the reporting in one of the following ways:

a) by making a recording of the conversation in a durable and retrievable form, subject to the consent of the whistleblower;
b) through a complete and accurate transcript of the conversation.

Where a telephone line or another voice messaging system where conversations cannot be recorded is used for reporting, the designated Team is required to draw up complete and accurate minutes in the form of a transcript of the conversation. The designated Team shall give the whistleblower the opportunity to check, rectify and agree to the minutes of the conversation by signing them.

If the whistleblower requests to report the breach in the presence of the designated Team, the latter is required to draw up minutes in a durable and retrievable form, subject to the consent of the whistleblower. The designated Team shall give the whistleblower the opportunity to check, rectify and agree to the minutes of the conversation by signing them.

If the whistleblower does not consent to the transcription or recording of the conversation, they shall be instructed to report to the designated Team in writing, on paper, or to send the report electronically to a dedicated e-mail address.

The 5 year period for record keeping also applies in the case of transcripts and minutes.

CHAPTER XII. WHISTLEBLOWERS' RIGHTS

A whistleblower enjoys the following rights, recognized by the specific legislation:

a) the right to freedom of expression;
b) the right to information;
c) the right to the protection of personal data;
d) the right to the confidentiality of their personal data and right to the protection of their identity;
e) the right to an effective remedy;
f) the right of defense;
g) the right to have their report examined and resolved in an objective manner, regardless of the convictions and interests of the Team designated for its resolution;
h) the right to be informed of the status of the follow-up no later than 3 months after the date when the receipt of the report was confirmed or, if the receipt of the report has not been confirmed, after the expiry of the 7 calendar days period calculated from the moment when the receipt should have been confirmed, and thereafter, whenever there are developments in the follow-up process, unless informing the whistleblower could jeopardize the follow-up;
i) the right to be informed on how the reported case will be resolved;
j) the right to receive the closure decision in cases where the reported case is closed;
k) the right not to be subjected to retaliation;

l) the right to receive a diligent and professional response to their request, within the legal deadline.

Whistleblowers' rights may not be waived or limited by a contract, regardless of its form or the terms of employment, including a pre-dispute arbitration agreement.

Any transaction intended to limit or waive rights provided for in this Policy is null and void.

Protection measures, support measures and remedial measures

Conditions

In order to qualify for the protection measures, the whistleblower must meet all the following conditions:

a) they are one of the persons who reported breaches internally within Autonom Services S.A. and who acquired information on breaches of law in a work-related context;
b) they had reasonable grounds to believe that the information on the breaches reported was true and that the report was necessary at the time of reporting;
c) they reported a breach internally within Autonom Services S.A. using the channel deployed at company level.

In order to qualify for the remedial measures, the whistleblower must meet all the above conditions, as well as the condition that the retaliation suffered must be a consequence of the reporting.

The measures provided for in this chapter also apply to:

a) facilitators;
b) third parties linked to the whistleblower who might suffer retaliation in a work-related context, such as colleagues or relatives of the whistleblower;
c) legal entities that the whistleblower owns or works for, or that are linked to the whistleblower in other ways in a work-related context;
d) a whistleblower who reports breaches to competent institutions, bodies, offices or agencies of the European Union.

In order to protect whistleblowers against retaliation, they benefit from remedial measures such as those previously provided for in this chapter.

A whistleblower who reports information on breaches of law does not violate the legal provisions or contractual terms related to the disclosure of information and is not liable for reporting or publicly disclosing such information, provided that the reporting or public disclosure was made in accordance with the legal provisions and that the whistleblower had reasonable grounds to believe that the reporting or disclosure was necessary in order to expose a breach of law.

The liability of whistleblowers for acts or omissions which are not related to reporting or public disclosure or which are not necessary for revealing a breach is subject to general provisions of law.

CHAPTER XIII. Prohibition of retaliation Challenging retaliatory measures

Any form of retaliation against whistleblowers is expressly prohibited, especially related to:

a) suspension or termination of the individual employment contract, of the employment relationship or of the collaboration contract signed with Autonom Services S.A.;
b) dismissal;
c) amendments to the employment contract, to the employment relationship or to the collaboration contract signed with the company;
d) reductions of the salary/allowance and/or changes in the working hours;
e) demotion or withholding of promotion and of professional development, including through negative individual performance reviews or negative recommendations related to the person's work;
f) imposition of any other disciplinary sanction;
g) coercion, intimidation, harassment or ostracism;
h) discrimination, disadvantaging the person in another way, or unfair treatment;
i) failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
j) failure to renew, or early termination of, a temporary employment/collaboration contract;
k) causing harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
l) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
m) early termination or cancellation of a contract for goods or services;
n) cancellation of a license or permit;
o) request for a psychiatric or medical evaluation.

Challenging retaliatory measures

The whistleblower may challenge the measures falling within the previously mentioned categories by means of a request addressed to the competent court with territorial jurisdiction over their place of residence. In such disputes, the burden of proving that the challenged measure is justified by reasons

other than those relating to the reporting or public disclosure lies with the Autonom Services S.A. company.

If the court finds that the measure against the whistleblower takes the form of retaliation following the reporting or public disclosure of a breach of law, it may order, as the case may be, the abolition of the measure, to restore the parties to their previous condition, the compensation of the damage, the termination of the measure and its prohibition in the future, as well as any other measures to stop any form of retaliation.

Even if there is no trial on the merits, the court may order, by means of a presidential order, the suspension of the previously mentioned measures applied to the whistleblower.

Upon taking any of the previously mentioned measures, the court shall, in all cases, also order the company to publish in a local or national newspaper, at its own expense, an extract from the decision by which it was found that a retaliatory measure was unlawfully imposed. The extract shall also be published on the existing website of the authority, of the company, as well as on the Agency's website, in compliance with the legislation on the protection of natural persons with regard to the processing of personal data.

If the court finds that the same whistleblower was subjected to retaliation at least twice for the same report or public disclosure, it may order, as the case may be, any of the previously mentioned measures against the employer, together with a civil fine of up to RON 10,000.

CHAPTER XIV. Conditions for disciplinary investigation

Disciplinary investigation shall be carried out in accordance with the conditions provided for in the updated Labor Code and the internal rules of the company.

The whistleblower shall benefit from all the rights set out in the specific legislation on disciplinary investigations and shall not be subject to arbitrary measures or decisions.

At the request of the whistleblower under disciplinary investigation as a consequence of internal reporting, disciplinary committees may invite the press and a representative of the trade union or professional association or a representative of the employees, as appropriate. The announcement shall be made by means of a notice on the website of the authority or the company at least 3 working days before the meeting, failing which the report and the disciplinary sanction applied will be considered null.

CHAPTER XV. Processing of personal data

Detailed information on the processing of personal data covered by this Policy can be consulted in the ***Information notice for data subjects on the processing of personal data in the context of reporting within AUTONOM, Annex no. 1 to this Policy.***

Annex No. 1 To the Whistleblowing procedure Information notice on the processing of personal data in the context of reporting within Autonom Services S.A.

AUTONOM SERVICES S.A. (hereinafter referred to as "**AUTONOM**"), headquartered in Mun. Piatra Neamt, Jud. Neamț, Str. Fermelor nr. 4, with the unique registration code (CUI) 18433260, hereby informs you about the processing of your personal data as a data subject and about the rights you have under the applicable legal provisions, i.e. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as "GDPR") and Legea nr. 190/2018 privind măsuri de punere in aplicare a Regulamentului 2016/679 (Law no. 190/2018 on measures implementing Regulation 2016/679).

1. Who processes the personal data?

AUTONOM SERVICES S.A. (hereinafter referred to as "**AUTONOM**", the **"Employer"** or the **"Company"**) acts as a personal data Controller.

Should there be any questions about the content of this information notice, the data subject is encouraged to send a written request to the management of the company, i.e. to the Data Protection Officer (DPO) appointed within AUTONOM, mentioning that they are an employee or collaborator of the company. The request shall be sent to the e-mail address: [...] or in writing, by post, to the following address: Mun. Piatra Neamt, Jud. Neamt, Str. Fermelor nr. 4.

Persons submitting such requests to AUTONOM are kindly asked to mention, in the subject of the email/on the mail envelope, information such as "**data protection Whistleblowing**", **"GDPR Whistleblowing"**, **"personal data reporting"**. This ensures that requests will be given priority.

As a data subject, you shall receive a response within 30 days from the moment when the document was submitted to AUTONOM. An extension of this deadline may only occur in exceptional situations. In such cases, we assure you that you will be properly informed of this deadline.

2. Purpose of the information notice

The aim of this document is to provide information on the processing of personal data in the context of reporting within AUTONOM, in accordance with the Whistleblowing Policy.

3. Definitions

a) **"Personal data"**: any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as their appearance, physical features, name and surname, etc.
b) **"Data subject":** whistleblower, data subject or third party in relation to AUTONOM, as defined in the Whistleblowing Policy.
c) "**Person concerned by the report**": the natural or legal person who is referred to in the report or public disclosure as a person to whom the breach of law is attributed or with whom that person is associated;
d) "**Whistleblower**": the natural person who reports or publicly discloses information on breaches of law which was acquired in a work-related context;
e) "**Report**": the oral or written communication of information on breaches within the company. Internal reporting is carried out using the means made available by Autonom Services S.A. for reporting breaches, as detailed below. These constitute the internal reporting channels;
f) "**Data Controller**" or "**Controller"**: AUTONOM SERVICES S.A., acting through the designated Team, which processes personal data via the internal reporting channel;
g) **"Processor"** means any natural or legal person, any public authority, any agency or any other body which processes personal data on behalf of a data controller or at the request of another Processor acting on behalf of a Data Controller;
h) **"Recipient"** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not;
i) **"Third party"** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;
j) "**Processing**": any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data acquired in the context of recording an internal report;
k) "**GDPR**": Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the Regulation).

4. Purpose of processing personal data

Personal data shall only be processed for specified, explicit and legitimate purposes, in accordance with Article 5 of the GDPR, and shall not be further processed in a manner that is incompatible with those

purposes. Personal data which are obviously not relevant to the processing of a particular report shall not be collected or, if collected accidentally, shall be deleted without undue delay.

The categories of data processed are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, and AUTONOM ensures compliance with the principle of data minimization.

Personal data will be processed, through the internal reporting channel described in the Whistleblowing Policy, for the purpose of fulfilling legal obligations and the legitimate interest of the Data Controller to prevent and manage breaches of legal provisions in the workplace or in the context of business partnerships.

AUTONOM assures data subjects that personal data, as described in this notice, will only be processed in strictly regulated situations and that the Operator will observe the right to life of any data subject.

5. Basis for the processing

Processing of data is carried out on the basis of ***point (c) of Article 6(1) of the GDPR***, as processing is necessary *for compliance with a legal obligation to which the controller is subject*. More specifically, it is carried out in order for AUTONOM to fulfil its obligation to implement an internal channel for reporting breaches in order to prevent any events having a negative impact on the data subjects and the company, to investigate such acts, but also to protect the staff, assets and activity of AUTONOM.

AUTONOM also processes personal data on the basis of ***point (f) of Article 6(1) of the GDPR***, specifically *on the basis of its legitimate interest*, reserving the right to prevent breaches of legal provisions, events likely to jeopardize the company's activity, as well as other situations that may have a negative impact on the controller and staff or collaborators.

6. Categories of data processed

When submitting a report, the categories of personal data that may be processed include, but are not limited to:

- name, surname, where applicable;
- pseudonym;
- position;
- email address;
- phone number;
- pictures of the data subject;
- voice;

- data contained in documents, files, audio-video recordings, etc. representing evidence;
- any other data made available to the designated Team by the whistleblower.

7. Categories of data recipients

AUTONOM shall not share the data processed as a result of reporting with third parties, but, in the event that an investigation reveals that a crime has been committed, the Operator shall take the necessary measures to contact the competent authorities and institutions and initiate legal proceedings.

AUTONOM guarantees to each whistleblower/data subject that the disclosure of personal data is made only on the basis of applicable legal provisions, and that the Operator makes every effort to ensure a secure data transfer.

! Note: In the event of an express request from criminal investigation bodies or authorities having jurisdiction to investigate breaches, the Operator shall make the requested data available to them for the purpose of preventing, investigating, detecting and prosecuting offences or enforcing sentences, including for the purpose of protection against threats to public safety and prevention of such threats.

8. International transfer of personal data

The personal data of the data subjects, processed as a result of reporting, will not be subject to international transfer, except in situations requiring such transfer.

9. Duration of storage of personal data

The duration of storage of the data obtained through the reports is 5 years, which is proportional to the purpose for which they are processed and complies with the legal provisions on the record-keeping of reports, except in situations expressly regulated by law or in duly justified cases.

10. Data subject's rights

In accordance with the GDPR Regulation, applicable from 25 May 2018, you have the possibility to exercise the following rights in relation to data processing, depending on the circumstances:

Note! In view of the internal reporting policy, data subjects cannot avail themselves of all the rights provided by the GDPR Regulation because, by the nature of the reports submitted and depending on the information actually sent to the designated Team by the person making the report, the content of the report cannot be changed.

- **RIGHT TO BE INFORMED**, set out in Articles 13 and 14 of the GDPR: This information notice provides all necessary information on the processing of personal data in the context of internal reporting carried out within AUTONOM. According to Article 14(3), the Controller shall provide information on the processing of personal data within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed. Last but not least, if a disclosure to another recipient is envisaged, the data subject will be informed at the latest on the date the personal data are first disclosed.
- **RIGHT OF ACCESS TO DATA:** According to Article 15 of the GDPR, you can request in writing a confirmation that your personal data are processed by AUTONOM and, where that is the case, you will be provided with a copy of these data as well as additional information about their processing.
- **RIGHT TO RECTIFICATION:** You can request the rectification of inaccurate, incomplete or amended personal data under Article 16 of the GDPR. Especially in the context of the reporting procedure, AUTONOM is not obliged to comply with a request for rectification of the data, in which case the refusal will be motivated.
- **RIGHT TO ERASURE:** Also in this case, given the particular nature of the internal reporting procedure, AUTONOM is not obliged to comply with a request for erasure of the data, in which case the refusal will be motivated.
- **RIGHT TO RESTRICTION OF PROCESSING** AUTONOM is not obliged to comply with a request for erasure of the data, in which case the refusal will be motivated.
- **RIGHT TO DATA PORTABILITY:** AUTONOM will not be able to comply with this request, in which case the refusal will be motivated.
- **RIGHT TO OBJECT:** AUTONOM is not obliged to comply with the request, in which case the refusal will be motivated.
- **RIGHT NOT TO BE SUBJECT TO A DECISION BASED SOLELY ON AUTOMATIC PROCESSING, INCLUDING PROFILING:** You may object at any time to a decision based solely on automated processing, including profiling, but only where that decision produces legal effects concerning you or affecting you to a significant extent. **In principle, the legal requirements for exercising this right are not met in the case of employment relationships within AUTONOM.** However, the controller provides the necessary means to exercise this right based on compliance with the requirements of the GDPR.
- **RIGHT TO LODGE A COMPLAINT:** According to Article 77 of the Regulation, you have the right to lodge a complaint with the National Supervisory Authority for Personal Data Processing ***(Mun. Bucharest, Bd. G-ral Gh. Magheru nr. 28-30, sector 1***) at any time, if you consider that the processing of personal data infringes the provisions of the Regulation, as well as the right to a judicial remedy.

Note! This information note was sent by AUTONOM in order to fulfil the information obligation that the company has as a personal data controller.

AUTONOM SERVICES S.A.