Whistleblowing System

Type of document : Procedure

P-0220

I: 01

Objective: The objective of this Procedure to explain the scope of the whistleblowing system and how it works for the Employees or Occasional and External Staff to safely report serious concerns without fear of retaliation. It describes the protection against any form of retaliation for anyone who speaks up selflessly and in good faith.

TABLE OF CONTENTS

1 Introduction

ArianeGroup is committed to strict compliance with laws and regulations and to high standard of ethical business conduct as reflected in the Ethics Charters[1][2], the Code of Conduct[3] and the Procedure for the Prevention of Corruption[4].

The Group is also committed to promote a group culture based on integrity, transparency, trust and respect for each-other. As such, the Company encourages speak up i.e. anyone should be allowed to express one-selves freely, and make report on what they perceive as suspected wrongdoings or violation of laws and external and internal regulations.

To this extent, ArianeGroup has defined a whistleblowing system, under the responsibility of its Group Ethics and Compliance Officer (GECO) for the employees or occasional or external staff to safely report serious facts (as defined in the present procedure) without fear of retaliation.

Because ArianeGroup encourages speak up, it does not tolerate any form of retaliation against anyone who speak up selflessly, on a substantiated basis, and in good faith.

The objective of this procedure is to explain the scope of the System and how it works, in compliance with the applicable laws and regulations [A1] [A2] [A3]. Safeguards have been implemented to protect data privacy as defined in the GDPR[5].

The present Procedure is applicable to the Employees of ArianeGroup and its Subsidiaries. Occasional and External Staff such as trainees, temporary workers and employees of service providers or subcontractors, can also use the System.

2 Optional and supplementary Nature

The use of ArianeGroup's System is not mandatory. As such, ArianeGroup will not take any action against Employees or Occasional and External Staff who do not use the System.

The System is supplementary to traditional channels of reporting concerns such as the immediate or indirect manager, or the Human Resources Business Partner (HRBP) and is not meant to replace those. Other local whistleblowing procedure may also exist in some foreign Subsidiaries.

Employees can continue to use these channels if they so wish. However, specific protective measures to safeguard confidentiality can only apply to Alerts lodged according to the present procedure.

Likewise, the System is not designed to replace similar means set up in companies employing ArianeGroup's Occasional and External Staff.

---

[1] Ethics Charter [D-0007-EFG] available on our website www.ariane.group and on the internal portal CMS
[2] Supplier Ethics Charter [D-0008-EFG] available on our website www.ariane.group and on the internal portal CMS
[3] Anticorruption Code of Conduct [D-0030-EFG] available on our website www.ariane.group and on the internal portal CMS
[4] Prevention of Corruption [P-0051-EFG] available on out internal portal CMS.
[5] General Data Protection Regulation (reference EU2016/679) 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 ("GDPR")

3 Definition and scope of an Alert

Making an alert consists into reporting, in good faith and selflessly the following serious facts:

- a criminal activity (felony or misdemeanour), or
- a serious and apparent violation of the law or regulations, or
- a serious threat or harm to public interest (relating to public health, safety or welfare), or
- potential or actual serious violation relating to human rights or fundamental liberties, or to health and safety or to the environment, or
- behaviour or situation contrary to the Code of Conduct or serious breaches of the Ethics Charter, or any other ethics and compliance policy and processes,

of which an Employee has personal knowledge, which has happened, is happening or is likely to happen, and relating to ArianeGroup, one of its Employees or one of its business partners.

In France, Employees can also report clear and serious violation of an international commitment duly ratified or approved by France, or of a unilateral act by an international organisation pursuant to such a commitment.

Reports can concern alleged facts of (i) corruption and influence peddling, or (ii) conflicts of interests, or (iii) fraud as well as of violations regarding (iv) competition and anti-trust, or (v) human rights and fundamental liberties, or (vi) environment, or (vii) health & safety.

The reporter must not reveal facts or documents containing classified information, nationally restricted or export controlled information as well as information covered by medical confidentiality or legal privilege.

Only a person acting in good faith and selflessly can be considered as a Whistleblower and benefit from the regime of the protection as prescribed by the law (See section 8 - Protection of the Whistleblower)

A person is considered to be acting "**in good faith**", when they provide information which they believe is comprehensive, fair and accurate, allowing them to reasonably believe in the truthfulness of the information given.

A person is considered as acting "**selflessly**", when they report an Alert without any expectations of financial compensation or gain.

Occasional and External Staff can also use the System to make Alerts when the reported situations result from ArianeGroup's activities, the activities of a third party with whom ArianeGroup has an established relationship, when such activities are related to such relationship.

ArianeGroup applies, as far as possible, the same methodology as when handling an Alert whether it comes from an Employee or from Occasional and External Staff.

4 Submitting an Alert

4.1 Recipient of the report

The Referent of the System, appointed by the President, upon approval by the Executive Committee, is the GECO.

A Deputy Referent is also appointed to represent the Referent in case he/she is absent or unable to act. Other Delegated Referents are nominated to process certain type of reports, relating either to a specific category or to a specific legal entity.

The reporter can submit their concern to the GECO by using the dedicated website https://arianegroup.1signal.net. This website is managed by an external provider bound by a strict confidentiality obligation and is secured to host and manage the data relating to the Alerts.

The contact phone number(s) to the Interactive Voice Recorder are communicated on the web platform.

4.2 Content and receiving of the report

The reporter describes, as objectively as possible and in detail, their concern. They should indicate when and how they became aware of the matter, to the extent of possible, provide all facts, information or documents, in digital form, which can help substantiate the report.

When describing the situation, the reporter must specify that these are alleged facts. Only information necessary to the evaluation of the report should be disclosed.

The reporter shall keep these information strictly confidential, unless the Referent is not evaluating diligently the admissibility of the Alert, as prescribed by the law.

As a reminder, the reporter must not reveal facts or documents containing classified or nationally restricted or export controlled information, as well as information covered by medical confidentiality or legal privilege.

The reporter should provide contact details to facilitate exchanges. The reporter will be required to confirm that they have read and agree to comply with the present procedure and that they have also been informed of the rules applicable to the processing of their personal data.

Once the form has been completely filled in, the reporter receives a receipt of completion. A confidential code is generated allowing the reported to communicate with the referents as necessary

The reporter is informed of the expected time necessary to examine the admissibility of the report within 30 working days.

4.3 Anonymous reporting

Anonymous reports are not encouraged. It is more difficult and sometimes impossible to examine anonymous reports or to establish whether the allegations are substantiated as well as to organise the protection of the reporter. In case of an anonymous report, the assessment of its admissibility and the appropriateness of its circulation within the present system will depend namely on the seriousness of the facts mentioned and the level of detail of the factual information provided.

If the anonymity renders it impossible to handle the report, the reporter will be informed via the anonymous dialogue box on the web platform.

4.4 Admissibility of the Alert

As a reminder, an Alert is admissible when it meets the following cumulative criteria:

- Reporter is a natural person, Employee or Occasional and External Staff
- Facts relates to the scope as defined in section 3 – Scope and Definition of an Alert
- Reporter has personal knowledge of the facts
- Reporting is made selflessly and in good faith.

The GECO or the Delegated Referent conducts, confidentially, a preliminary analysis of the report, before ruling on its admissibility. The reporter may be asked to provide further information.

After this analysis, the GECO or the Delegated Referent notifies the reporter of the admissibility or non-admissibility of the Alert, using the secured dialogue box on the web platform. If the alert is not admissible because it falls outside the scope of the present policy, the reporter will be informed and, where possible, advised on possible alternate channels allowing their concern/grievance to be addressed.

Subject to document retention requirements of local legislation, the elements of the report are deleted within a maximum delay of 2 months from the non-admissibility decision (except if the report results in a disciplinary or judicial proceedings).

5 Handling the Alert

Once it is confirmed the alert falls into the scope, the GECO or the persons he/she appoints will be handling internally the alert, according to the internal process of handling Alerts. If necessary, the GECO may constitute an investigation team made of Delegated Referents, Authorised Contributors or External Contributors.

The handling of the Alert complies with the applicable legislation. It is handled neutrally, without any bias for parties involved, respectfully of the presumption of innocence.

The person implicated by the alert will be informed of the nature of the allegations and of the name of the person handling the report. This information may not be provided immediately should it prove necessary, for example, to check facts, preserve evidence, protect individuals or contact the local authorities.

The reporter and the person implicated by alert are informed when the handling of the Alert is concluded. To the extent possible, they are informed of the conclusions. The need for confidentiality or legal requirements or the protection of individuals may prevent from being shared, the specific details of the Alert, its handling or any measures taken as a result.

All Alerts are handled by the Referent, supported as relevant by an, investigation team, respecting the following fundamental principles

- Confidentiality
- Whistleblower protection
- Presumption of innocence of people implicated in the Alert
- Respect for Privacy
- Respect for medical secret, defence secret and legal privilege.

6 Confidentiality

Authorised persons and persons handling reports are bound by a strict confidentiality obligation.

The elements allowing the identification of the reporter cannot be divulged, except to the legal authorities, without their consent. If their refusal makes it impossible to handle the Report, the reporter is so informed.

The identity of the reporter, the subject matter of the Alert and the identity of the persons implicated can only be shared by the GECO, the Deputy Referent, the concerned Delegated Referents or any other member of the investigation team ("Authorised Contributors") in order to handle the report or to take appropriate measures. These persons are bound by a strict confidentiality obligation.

Specific measures are taken to ensure confidentiality during the handling of the Alert (written reminder of confidentiality rules and possible sanctions in case of non-compliance, secure emails etc…). In particular, the access to information is organised according to the need to know basis, using a personal log-on and password to the platform as well as a unique ID to each connection.

Each Authorised Contributor commits to respect the internal procedure and to confidentiality, neutrality and impartiality. When the handling of an Alert requires the support of External Contributors, they should commit contractually not to use personal data for other purpose than those for which it was collected, to ensure their confidentiality, destroy or restore these personal data at the end of the processing.

Any information shared in relation to the handling of the Alert is deemed confidential and shall be protected by anyone who gets access to such information.

The identity of the reporter of an Alert and as applicable, the person(s) implicated in the Alert may be communicated to the judicial authority at their request.

Subject to document retention requirements of local legislation, the elements of the Alert (as defined in section 8.1 – data processed) will be deleted or archived within a maximum delay of 2 months after the handling of the Alert is concluded. If the Alert processing results in in disciplinary or legal proceedings, elements relating to this Alert may be retained for the duration of the proceedings, until the prescription of the right to appeal such decision.

7 Whistleblower Protection

According to the law, an Employee cannot be sanctioned, dismissed or discriminated against, for having reported an Alert selflessly and in good faith, even if later the facts are proven false or are not followed up, or for having participated in the Alert handling. A Whistleblower which has reported an Alert selflessly and in good faith cannot be excluded from a recruitment process, access to an internship or to professional training.

Any direct or indirect Retaliation towards an Employee who have submitted an Alert will not be tolerated. Anyone who think they are subject to Retaliation for having submitted an Alert or participated in its handling can contact the GECO.

Any retaliatory acts or threats by Employees can give rise to disciplinary sanctions, subject to local regulations.

The Whistleblower protection can only benefit to those acting selflessly and in good faith as described in section 3 – Scope and Definition of an Alert, without harming ArianeGroup.

8 Personal Data Protection

The System is compliant with the GDPR and applicable national laws and regulations [A4] [A5] [A6].

8.1 Data processed

When an Employee or an Occasional and External Staff raises an alert, they may communicate to ArianeGroup personal data about them, as well as, personal data about person(s) targeted or about person(s) able to provide information necessary for processing the Alert.

Personal data that can be collected and processed include in particular:

- the identity, function and contact details of the reporter,
- the identity, function and contact information on the person(s) implicated by the report;
- any other information voluntarily communicated by the reporter, or
- resulting from the processing of the alert.

When handling an Alert, ArianeGroup may also collect personal data concerning person(s) who may provide information necessary for the handling of the Alert (these persons may have been identified by the reporter or not).

8.2 Purposes

Personal data is collected and processed for the purposes of assessing the admissibility of the Alert, of checking facts and taking appropriate measures, if necessary. It enables ArianeGroup to comply with its legal obligations [A1] [A2] [A3] and to protect its legitimate interests[6]

8.3 Data Controllers

ArianeGroup SAS is the Data Controller of the personal data collected and processed.

When handling an Alert, personal data may be collected or processed by, or transferred to other entities of the Group, for example, the entity where the relevant Employee is employed. In that case, such company shall be considered as Data Controller as well.

All the Group's companies process personal data according to the detailed requirements of this proceeding.

8.4 Retention period

Refers to the section 4.4 – Admissibility of the Alert and section 6 – Confidentiality.

8.5 Recipients

Persons who may have access to the personal data provided or collected are the GEGO, the Authorised Contributors and more generally all those persons who may participate to the data processing as part of (i) the collection or/and the processing of the report or (ii) to take appropriate measures, in accordance with the Procedure. These might include persons within ArianeGroup or its Subsidiaries.

[6] See (1), (2), (3) and (4)

The external provider in charge of the web platform is also a recipient.

All these persons are subject to a strict confidentiality obligation as described in section 6 - Confidentiality

8.6 Data Subjects rights

Any person whose personal data is collected and processed, in the framework of the Alert processing, has the following rights:

- the right to access in their personal data, which means to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to the personal data with some specific information on its processing (in compliance with the applicable legislation);
- the right to rectify inaccurate or incomplete personal data ;
- the right to ask for personal data to be deleted, also called « right to be forgotten », which allow data subject to obtain the deletion of their personal data in certain conditions (ex: personal data is no longer necessary for the processing of follow up of an Alert) , subject to potential legal obligations of retention;
- the right to restrict the processing of the personal data (including, in some cases, to obtain the suspension of the processing);
- the right to object to the processing of their personal data for reasons relating to their particular situation. However when the reporter refuses the collection or processing of their personal data, it can make difficult or even impossible to handle an Alert. Furthermore, this right to object cannot be used to prevent the Company to fulfil its legal obligations concerning the processing of the Alert and the protection of the Whistleblower;
- the right to give instructions about the preservation, the deletion and the communication of their personal data after their death ;
- the right to lodge a complaint with the relevant supervisory authority, especially in the European Union member state of their habitual residence, workplace, or where the alleged breach of the applicable regulations occurred.

For the exercise of this rights, refer to the applicable Information Notice [A9].

9 Definitions

Alert	Any report which meet the following conditions: ▪ Reporter is a natural person, Employee or Occasional and External Staff ▪ Facts relates to the scope as defined in section 3 – Scope and Definition of an Alert ▪ Reporter has personal knowledge of the facts ▪ Reporting is made selflessly and in good faith.
ArianeGroup	Refers to ArianeGroup Holding, ArianeGroup SAS and ArianeGroup GmbH

Authorised Contributors	Person who is invited by a referent to help handle a specific Alert. The access to the Alert details is subject to the prior signing of a confidentiality commitment and approved by an authorisation letter.
Delegated Referent	Employee who is a recipient to specific report and participates to the handling of the Alerts within a pre-defined perimeter, for example, he/she dedicated to one or several categories or to reports which relates to one or several legal entities. The Subsidiary Compliance Officer (SCO) can be appointed Delegated Referent by the President of the said legal entity, subject to prior approval of the GECO.
Deputy Referent	Appointed by the President of ArianeGroup Holding, he/she represents the Referent in case he/she is absent or unable to act
Employees	▪ All employees, officers or directors of ArianeGroup or its Subsidiaries, whether working full-time or part-time, for an indefinite-term or fixed-term with a valid labour contract at the time of disclosure ; ▪ Subject to statute of limitation requirements of local legislation, Employee having left the Group, when making their report at the latest within 2 months of their last day of actual work
GECO	Group Ethics and Compliance officer
Group	ArianeGroup Holding SAS, ArianeGroup SAS and ArianeGroup GmbH and their Subsidiaries
Occasional and External Staff	Any natural person who collaborates professionally with the Group. Occasional Staff includes for example interns. External Staff are individuals employed by a third party with whom the Group has an established relationship. They include for example temps, or employees of suppliers or of subcontractors.
Referent	Is the main recipient of reports and manages under his/her sole responsibility the handling of the Alerts. ArianeGroup's Referent, appointed by the President of ArianeGroup Holding, and approved by the Executive Committee is the GECO
Retaliation	Means excluding a person from a recruitment process or access to an internship or professional training program as well as disciplining, dismissing or threatening them, subjecting them to other unfavourable treatment or taking discriminatory measures against them with regard to nature of duties, compensation, profit-sharing, share allocation, training, redeployment, qualifications, classification, promotions, transfers or renewal of employment or temporary work contract. Harassment and bullying actions can also, depending on the facts and circumstances, be considered retaliation.

Subsidiary	Legal entity in which ArianeGroup Holding, directly or indirectly, holds more than 50% of the shares and/or voting rights.
System	Refers to the unique whistleblowing system designed to collect reports as described in the present procedure.

10 Categories

Competition	Violation of regulations relating to competition and anti-trust. Unauthorised access to company confidential information.
Conflict of Interest	A situation in which an employee's individual interests interfere, or appear to interfere, with his/her ability to perform loyally his/her job
Corruption and Influence Peddling	▪ Giving, offering, promising (active corruption) or soliciting or receiving (passive corruption) money, a service or anything of value in order to unduly influence someone to take, delay or refrain from taking an action within the scope of his/her professional duties. ▪ Situation or behaviour likely to contradict the Code of Conduct
Fraud	Misstatements or omissions in accounting records and financial statements that are designed to deceive the users of such information, misappropriation of assets by dishonestly appropriating, concealing or misusing the company's assets, and violation of anti-money laundering laws
Health and Safety, Environment (HSE)	Any situation which present a risk of serious harm to the health or safety of individuals, as well to environment as a result of the company's activities
Human Rights and Fundamental Liberties	Allegations of violation of internationally recognized standards in the field of human rights and fundamental liberties as defined the Universal Declaration of Human Rights, the United Nations Guiding Principles on Business and Human Rights, and the International Labour Organization Declaration on Fundamental Principles and Rights at Work, within the group and its supply chain.
Other Laws and Regulations	Allegations of serious violations of other laws and regulations. Includes Retaliations against a person who have reported an Alert or participated in its handling

11 Reference Documents

[A1] Act No. 2016-1691, of 9 December 2016, relating to Transparency, Anti-Corruption and Economic Modernisation
[A2] Decree No. 2017-564, of 19 April 2017, relating to the procedures for collecting the report from Whistleblowers within private and public sector organisations
[A3] Act No. 2017-399, of 27 March 2017, relating to the duty of vigilance of parent companies and contracting companies
[A4] Act No. 78-17, of 6 January 1978, relating to data processing, computer records and freedom, as modified by the law dated 6 August 2004
[A5] Framework from the French Data Privacy Authority (*Commission Nationale Informatique et Liberté* – CNIL) regarding the processing of personal data in implementing a whistleblowing system.
[A6] Federal Personal Data Protection Act of 30 June 2017 (BDSG – German abbreviation for Bundesdatenschutzgesetz)
[A7] 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.
[A8] Personal Data Protection [P-0010
[A9] Data Privacy Information Notice relating to the Whistleblowing System (version 1, December 2020)