WHISTLEBLOWING POLICY

For the Altrad Group *(hereafter "the Group")*, integrity is an essential condition for conducting business, not only because national and international regulations have increased the risks and negative consequences of illegal or illicit behaviour, but also because integrity helps to ensure the Group's stability and sustainability.

The Altrad Group defines itself by its values of **respect, courage, solidarity, humility** and **conviviality**, values which are inseparable from its success. All Altrad Group activities must be conducted in a transparent and ethical manner and in accordance with the laws of each country in which the Altrad Group is present.

The whistleblowing system is part of the compliance programme deployed by the Altrad Group. It ensures the effectiveness of the procedures deployed and is a legal obligation under:

- Act no. 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life, known as the "Sapin II Act";
- the UK Bribery Act of 8 April 2010, known as the "UKBA";
- Act no. 2017-399 of 27 March 2017 on the duty of care of parent companies and ordering companies;
- European Directive 2019/1937 of 23 October 2019 on the protection of persons who report breaches of Union law.

The purpose of this policy is to:

- define the scope of the warning system;
- set out the terms and conditions of its operation;
- present the guarantees offered by this scheme;
- set out the conditions for the use and storage of personal data collected under the scheme.

The Altrad Group undertakes to analyse the admissibility of all reports received, to carry out an investigation where necessary and, in any event, to ensure the confidentiality of the procedure. The present policy enables all employees and partners working for or with the Altrad Group to make a report, in complete confidentiality, without fear of reprisals.

The Altrad Group Ethics Committee is responsible for the application of and compliance with this policy. Group management is responsible for ensuring that employees and partners understand and comply with this policy and receive appropriate and regular training on this subject. The Chief Compliance Officer of the Altrad Group is responsible for implementing this policy with the assistance of the Head of Compliance, the Compliance Department, Altrad Group management and the Local Compliance Officers *(hereinafter "LCOs")*.

The Altrad Group reserves the right to modify this policy at any time without prior notice.

Date	Type	Editor	Approver	Review
01/09/2020	Creation	ET	RO	1
17/06/2024	Modification - adaptation to legislative changes	CS	ET	2
18/07/2024	English translation	CS	PM	2

Table of contents

1 Scope of the whistleblowing system

1.1 What facts can be the subject of an alert?

A whistleblowing report is the disclosure to the Altrad Group of information relating to suspected workplace hazards or wrongdoing by or against employees of the Altrad Group.

In order to constitute an alert, the facts reported must be of a material nature:

- a crime or misdemeanour ;
- an infringement or an attempt to conceal an infringement:
  - an international commitment
  - a unilateral act of an international organisation taken on the basis of a duly ratified international commitment
  - European Union law
  - a law or regulation
- a threat or harm to the public interest;
- a breach/behaviour or situation contrary to the Altrad Group Code of Integrity and Ethics.

These may include, but are not limited to:

- corruption or influence peddling ;
- endangering the health and/or safety of employees;
- financial fraud or mismanagement ;
- criminal activities;
- environmental damage;
- behaviour likely to damage the reputation of the Altrad Group;
- unauthorised disclosure of confidential information;
- any behaviour that is disrespectful or contrary to human dignity (for example: ethnic, gender, religious or cultural discrimination contrary to the Group's values and its diversity and inclusion policy);
- a practice of labour exploitation that jeopardises human dignity and rights.

Items reported via the alert system must always be:

- factual and directly related to the subject of the alert;
- objectively formulated;
- strictly necessary to verify the alleged facts or to process the alert and proportionate to the protection of the interests in question.

In any event, the alert is issued without malice or intent, in the pursuit of the general interest and not the satisfaction of any personal interest, financial or otherwise, with a view to putting an end to a dangerous situation or other reprehensible acts.

Facts, information or documents, whatever their form or medium, covered by national defence secrecy, medical secrecy, the secrecy of judicial deliberations, the secrecy of investigations or judicial enquiries and the professional secrecy of lawyers are excluded from the scope of the whistleblowing system.

1.2 Who can issue an alert?

The alert system can be used by:

- all Group employees and managers, whatever their position or status (including external and occasional employees);
- former Group employees and managers;
- people who have applied for a job within a Group entity;
- shareholders, associates and holders of voting rights at the Group General Meeting;
- members of the Group's administrative, management or supervisory bodies;
- all external stakeholders interacting with the Group, such as customers, co-contractors, suppliers, intermediaries, business introducers, certification bodies, subcontractors, etc.

To be recognised as a whistleblower, the author of an alert must:[1]

- be a natural person;
- act in good faith;
- report without direct financial compensation[2];
- report or disclose information that falls within the scope of the whistleblowing system *(see above)*.

2 How the whistleblowing system works

2.1 How do I send an alert?

Misconduct, inappropriate situations and behaviour, as well as evidence to support the allegations made, can be reported via a number of channels, as detailed below.

It is possible to submit an alert anonymously. However, we strongly encourage whistleblowers to identify themselves so that the people in charge of handling alerts can come back to them to obtain further information, keep them informed and be able to protect them against possible reprisals.

2.1.1 Talking to your line manager

Most of the time, you can raise your concerns with your line manager. This can be done in person or in writing. In some cases, he or she will be able to resolve the problem quickly and effectively.

This report may be made by telephone or any other voice mail system. The person making the report may also request a face-to-face meeting or a videoconference, organised no later than twenty working days after receipt of the request.

Alerts received through the chain of command are forwarded to the LCO so that they can be integrated into the GAN alert management platform.

[1] These conditions are cumulative.

[2] Whistleblowers receive no direct financial benefit and are not remunerated for their actions.

2.1.2 Contact the Compliance Department or the LCO

If the whistleblower feels that it would be inappropriate to discuss the matter with their line manager, or if their line manager has not responded to their concern, they can use one of the following channels:

- contact the Local Compliance Officer;
- submit a report online via the Altrad Group Compliance platform: https://*altrad.gan-compliance.com/*;
- send an email to the Compliance department: compliance@altrad.com.

2.1.3 Use the Whistleblowing platform

The Altrad Group Whistleblowing Platform can be accessed via the following link: https://altrad.gan-compliance.com/caseReport.

If the person submitting the alert has a GAN account, they can submit their alert without logging in, in order to submit an anonymous alert.

2.1.4 Call the Hotline

Reporters may also prefer to use the telephone alert line.

The telephone number is available on GAN and on the warning system posters displayed in all Altrad Group company workplaces.

2.1.5 External reporting

In accordance with Act no. 2022-401 of 21 March 2022 aimed at improving the protection of whistleblowers, whistleblowers may also choose to use the external channel by contacting directly the "Défenseur des droits", the administrative or judicial authority or the competent European Union institution, body or agency.

If the alert is not dealt with within a reasonable period of time, and only as a last resort, the author of the alert may publicly disclose the facts that are the subject of the alert. This option is only available to whistleblowers in the event of serious and imminent danger[3] and if referring the matter to an authority would entail a risk of reprisals against the whistleblower or would not make it possible to remedy the matter effectively in view of the particular circumstances of the case.

Before reporting any concerns to an external body or person, we strongly encourage the reporter to seek advice and exhaust internal channels first, taking into account any confidentiality obligations that may apply.

2.2 Who collects and analyses reports?

Reports are centralised in the GAN alert management platform and are received by the Head of Compliance and the Regional Compliance Officers. The recipients of alerts are required to respect the strict confidentiality of this information, which in any event is only used for the purposes of analysing, processing and investigating the alerts.

The Compliance department acknowledges receipt of the alert to the author of the alert, when the latter is identified and/or contactable, within seven working days of receipt. Acknowledgement of receipt is sent in writing via the GAN alert management platform and does not constitute acceptance of the alert.

[3] The "imminent and manifest" danger to the public interest also justifies the person making the alert disclosing the facts that are the subject of the alert publicly if this information was obtained in the course of his or her professional activity, particularly when there is an emergency situation or a risk of irreversible harm.

3 Procedures for handling alerts

3.1 Examination of the admissibility of alerts

The first stage in processing an alert is to analyse its admissibility. The Head of Compliance carries out a preliminary analysis to determine whether the alert falls within the scope of the whistleblowing system (*see above*).

If the information provided is incomplete or insufficient, the Compliance department may request additional information from the author of the alert in order to determine whether it is admissible.

To be admissible, the alert must fall within the scope of the alert system and include:

- a precise description of the events observed;
- the name and position of the person concerned by the alert;
- where appropriate, supporting documents to substantiate the allegations made.

If the preliminary analysis shows that the alert does not fall within the scope of the whistleblowing system, or if the information provided is not sufficient to enable an investigation to be carried out, the Head of Compliance will declare the alert inadmissible. The Head of Compliance will explain the reasons for the inadmissibility of the alert to its author and the personal data collected as part of the alert will be anonymised without delay.

On the other hand, if the preliminary analysis shows that the alert falls within the scope of the whistleblowing system, the Head of Compliance will inform the person making the alert that it is admissible and of the reasonable and foreseeable time required to investigate the allegations made.

3.2 Alert instruction

The Regional Compliance Officers appoint, via GAN, the investigator who will be responsible for shedding light on the facts that are the subject of the alert. Depending on the nature of the allegations, the persons concerned by the report and the skills required to carry out the internal investigation, the following people may be appointed as investigators:

- the Local Compliance Officer of the subsidiary concerned;
- the Managing Director of the subsidiary concerned;
- the Group Human Resources Director or the HR manager of the subsidiary concerned;
- the Health, Safety & Hygiene Officer of the subsidiary concerned;
- a member of Internal Audit;
- external advice (law firm, forensic specialist, consultants).

The Compliance department always ensures that the appointed investigator has no conflict of interest, is able to conduct the investigation impartially and respects the confidentiality of the procedure.

The investigator shall inform, within a reasonable period of time which may not exceed one month[4] , the person concerned by the facts that are the subject of the alert by the means that they consider to be the most appropriate and shall inform them of the alert policy. In any event, this information shall not include any information that would enable the person making the alert to be identified.

The investigator will carry out all the investigative steps that they consider necessary and appropriate in order to shed light on the facts that are the subject of the alert, in compliance with the applicable social legislation. They will interview the person who reported the matter, the person who is the subject of the alert and any witnesses to corroborate or refute the allegations made in the alert. Minutes are taken of these interviews and archived to document the investigation of the alert.

[4] This information may be deferred if there is a risk that it will compromise the proper handling of the alert, particularly if there is a risk of destruction of evidence justifying the taking of precautionary measures. The person concerned by the facts that are the subject of the alert will then be informed of the holding of an investigation as soon as this risk is eliminated.

The investigator shall inform the author of the alert, within a reasonable period of time not exceeding three months from the acknowledgement of receipt of the alert, of the measures envisaged or taken to assess the accuracy of the allegations and, where appropriate, to remedy them, as well as the reasons for these measures.

3.3 Closing the alert

The investigation phase concludes with the investigator drafting an investigation report. This report describes the facts that are the subject of the alert and analyses them from a legal point of view. It details the investigation carried out, the information gathered to confirm or refute the allegations, the actions and any disciplinary measures recommended to remedy the facts that are the subject of the alert. This report is submitted to the Compliance department for validation, and the Compliance department, in conjunction with members of the management team, implements the actions required to resolve the alert. The investigator informs the author of the alert and the person concerned in writing of the closure of the procedure and the action taken before closing the alert on the alert management platform.

The investigator may decide, in conjunction with the Compliance Department, to inform the administrative or judicial authorities of the conduct revealed by the investigation, if this is justified by the results of the internal investigation.

4 Guarantees offered by the alert system

The Altrad Group understands that potential whistleblowers may be concerned about the possible repercussions of reporting. We are committed to supporting all Group employees who raise genuine concerns under this policy, even if it turns out that they were mistaken.

4.1 Confidentiality

The Altrad Group takes all necessary measures to guarantee the strict confidentiality of the facts that are the subject of the alert, the identity of the person making the alert, the persons targeted by the alert and any third party mentioned in the alert, as well as the information collected as part of the investigation. Any breach of the confidentiality of the procedure may result in disciplinary sanctions and legal proceedings.

We guarantee that the whistleblower's identity will remain strictly confidential and will not be disclosed (except to the judicial authorities where this is mandatory) unless he or she has given his or her express consent.

The identity of the persons concerned by a warning is not disclosed (except to the judicial authorities) until it has been established that the warning is well-founded.

4.2 Protection against reprisals

The author of a whistleblowing report who has exercised his or her right to report in good faith and without receiving any direct benefit (even if the facts reported subsequently prove to be inaccurate or do not give rise to any follow-up), benefits from legal protection against any form of reprisal[5] . Any Altrad Group employee involved in reprisals against a whistleblower will be subject to disciplinary measures.

[5] In particular, the following measures: suspension, lay-off, dismissal or equivalent measures; demotion or refusal of promotion; transfer of duties, change of place of work, reduction in salary, change in working hours; suspension of training; negative performance appraisal or work certificate; disciplinary measures imposed or administered, reprimand or other sanction, including a financial penalty; coercion, intimidation, harassment or ostracism; discrimination, disadvantageous or unfair treatment; failure to convert a fixed-term employment contract or a temporary contract into a permanent contract, where the employee had a legitimate expectation of being offered permanent employment; non-renewal or early termination of a fixed-term employment contract or a temporary contract; damage, including damage to the person's reputation, in particular on an online public communication service, or financial loss, including loss of business and loss of income; blacklisting on the basis of a formal or informal agreement at sector or industry level, which may imply that the person will not be able to find future employment in the sector or industry; early termination or cancellation of a contract for goods or services; cancellation of a licence or permit; undue referral for psychiatric or medical treatment.

This protection also applies to whistleblowing facilitators[6] , to natural persons in contact with the whistleblower who are at risk of reprisals in the course of their professional activities (from their employer, client or the recipient of their services) and to legal entities controlled by the whistleblower, for which he or she works or with which he or she is in contact in a professional context.

However, any misuse of the whistleblowing system, in particular constituting slanderous or insulting denunciation, may expose the perpetrator to disciplinary sanctions and legal proceedings.

4.3 Civil and criminal liability

A whistleblower who has exercised his right to alert in good faith and without any direct benefit (even if the facts reported subsequently prove to be inaccurate or do not give rise to any follow-up action) is not liable under civil or criminal law. They cannot be held liable for damage caused by their whistleblowing if they had reasonable grounds for believing that the information was necessary to safeguard the interests in question.

This protection also applies to the whistleblower's facilitators, to natural persons linked to the whistleblower who are at risk of reprisals in the context of their professional activities (from their employer, client or the recipient of their services) and to legal entities controlled by the whistleblower, for which he or she works or with which he or she is linked in a professional context.

5 Protection of personal data

5.1 Who is the data controller and who has access to the data?

The Altrad Group is responsible for the processing[7],[8] of personal data[9] collected as part of the alert system. In this context, the Group undertakes to comply with European Union Regulation 2016-679 of 27 April 2016 known as the "RGPD" and Law No. 78-17 of 6 January 1978 known as the "Informatique et Libertés" law in its latest version in force.

The Altrad Group takes all necessary precautions to preserve the security of personal data, in accordance with the Recommendations of the *Commission Nationale de l'Informatique et des Libertés* (CNIL), in order to prevent the data collected from being distorted, damaged or accessed by unauthorised third parties.

Personal data may only be accessed by persons authorised to have access to it by virtue of their functions, namely:

- the recipient of the alert;
- in the event of a telephone report, the staff of the WBS service provider;
- the Compliance department;
- the appointed investigator;
- as part of maintenance operations, staff from the GAN alert management platform;
- members of management and, where appropriate, of the human resources department, who are involved in implementing measures to remedy the facts that are the subject of the alert;
- where appropriate, the external advisor (law firm, forensic specialist, consultants) involved in handling the alert or following up the investigation.

---

[6] A facilitator is an individual or association that helps a whistleblower to make a report in compliance with the law.

[7] The term "controller" refers to the legal or natural person who determines the purposes and means of a processing operation, i.e. the objective and the way in which it is carried out.

[8] The term "processing" refers to any operation, or set of operations, relating to personal data, regardless of the process used (collection, recording, organisation, storage, adaptation, modification, retrieval, consultation, use, disclosure by transmission or dissemination or any other form of making available, alignment).

[9] The term "personal data" refers to any information relating to an identified or identifiable natural person.

5.2 What data is collected and why?

The purpose of the whistleblowing system is to identify and deal with breaches of the law and of the Code of Ethics and Business Integrity *(see above)*. In this context, the information likely to be collected via the whistleblowing system is:

- the facts reported;
- the identity, functions and contact details of the person making the alert, the persons concerned by the alert, the persons involved, consulted or heard in the collection or processing of the alert and the facilitators or persons in contact with the person making the alert;
- information gathered in the course of verifying the facts reported;
- audit reports;
- the action taken in response to the alert.

The Altrad Group only processes personal data that is communicated to it insofar as it is strictly necessary for the analysis and investigation of the facts that are the subject of the alert, in the context of related legal proceedings, or to comply with a legal obligation. In any event, personal data is processed solely for the purposes of the internal alert.

In certain exceptional circumstances, the Altrad Group may be required to disclose personal data:

- if we are legally obliged to disclose the identity of the whistleblower; *or*
- if we are legally authorised to disclose the identity of the whistleblower in order to protect or defend the rights of the Group or those of our employees, customers, suppliers or partners.

5.3 How long is personal data kept?

The Altrad Group only retains personal data collected as part of the alert system for the time strictly necessary and proportionate to its processing and the protection of its authors, the persons it concerns and the third parties it mentions, within the limits of the retention periods provided for by the applicable regulations.

When the Head of Compliance declares a report inadmissible, the Altrad Group immediately anonymises the personal data relating to the report.

When the alert is admissible but does not give rise to any follow-up (any decision taken by the Altrad Group to draw conclusions from the alert), the personal data linked to the alert is made anonymous within two months of the end of the investigation.

When disciplinary or legal proceedings are initiated against the person who is the subject of the warning or the person who has made the warning, in the event of misuse of the warning system, the Altrad Group will keep the personal data collected in the context of the warning until the end of the proceedings and the time limit for appealing against the decision. At the end of this period, the Altrad Group will make the personal data anonymous.

5.4 What rights do people whose personal data has been collected have?

The Altrad Group guarantees any person whose personal data has been collected as part of the alert system the **right to access** the data concerning them and the possibility of requesting, if it is inaccurate, incomplete, ambiguous or out of date, that it be **rectified within** the legally prescribed time limits, in accordance with the applicable regulations.

Any person whose personal data has been collected as part of the whistleblowing system may also request that the processing of their personal data be **restricted** if it is inaccurate, or that their personal data be **deleted** if it is no longer necessary for the purposes for which it was collected, or if it has been processed unlawfully or to comply with another of the Group's legal obligations.

Any person whose personal data has been collected as part of the alert system also has the right to **object to** their data being processed if they cite reasons relating to their particular situation. However, the Group may not comply with this request if there are legitimate and compelling reasons for processing the data, or if the data is necessary for the establishment, exercise or defence of legal claims, or if the processing of the data is subject to a legal obligation.

To exercise any of your data protection rights, send an email to compliance@altrad.com. If you are not completely satisfied with our response to your complaint or if you consider that the processing of your personal data does not comply with data protection legislation, you may lodge a complaint with the competent authority responsible for the protection of personal data in the country in which you are established. The contact details of each European authority responsible for the protection of personal data are available at the following address: https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm

6 Checks and monitoring

The Compliance Department carries out regular checks to ensure that the whistleblowing system is appropriate and effective. The purpose of these checks is to evaluate the implementation of the whistleblowing system, identify and understand any breaches and improve the effectiveness of the compliance programme. The controls may, among other things, cover the verification of communication actions relating to the whistleblowing system, compliance with the Internal Investigation Procedure by investigators and the absence of retaliatory measures against the whistleblower.

A report on the whistleblowing system (key indicators, processing results, average processing times, types of cases reported) is drawn up by the Head of Compliance and presented to the Group Ethics Committee every year.

Appendix - Examples

Internal Alert	You meet a colleague in a Michelin-starred restaurant with a customer, during a tender procedure. Talk to the LCO or report it via the alert system.
	Scaffolding has not been erected in accordance with the rules and the calculation note. Contact your line manager or the HSE representative. If no action is taken, you can use the warning system.
	You notice suspicious payments validated by your line manager. Report it via the alert system.
	Your work colleagues make comments that make you feel uncomfortable about your gender, religion, sexual orientation or origins. Speak to the HR department about it, and if they don't reply, use the alert system.
	A colleague asks you to carry out an operation that does not appear to be legal or ethical. Report it via the alert system.
	A sales representative is using practices that contravene competition law. Report it via the alert system.
	You notice that purchases made by your company are being made from a new service provider, who is a member of the Director's family. Report this via the alert system.
Not an Internal Alert	You had an argument with a colleague at lunchtime. You report the matter to your line manager. This is not an internal alert.
	You notice errors on your payslip. This is not a warning. Contact the Human Resources department.
	Your colleague tells you that the branch manager has just bought himself a luxury car with company money. This is not an internal alert but a rumour.
	During the coffee break, you hear that the secretary is having an intimate relationship with one of the directors. This is not a warning, but an inappropriate rumour.
	Your instinct, which is never wrong, is that your new colleague is not very clean-cut. This is not a reason for an internal alert.