INTERNAL WHISTLE-BLOWING SYSTEM
SIFCOR Group
January 2020

The SIFCOR Group is implementing an anti-corruption programme in accordance with the SAPIN II law from January 2020. It covers all its subsidiaries and concerns all its employees, customers, suppliers and partners.

Please find below, the internal whistle-blowing system of the SIFCOR group that applies to AMIS.

This document is structured as follows:

****

I. Applicable rules

1. Legal basis

The French law n°2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life, known as the "Sapin 2 law", requires the implementation, for companies employing at least 500 employees (or belonging to a group whose parent company has its registered office in France and whose workforce includes at least 500 employees), and having a turnover exceeding 100 million euros (social or consolidated), of an anti-corruption compliance programme (Article 17 of the law).

This programme includes 8 preventive measures, including an internal whistle-blowing system.

In addition to this anti-corruption whistle-blowing mechanism, the law provides that companies with at least 50 employees are also required to set up a procedure for collecting reports issued by their employees or by external and occasional collaborators (Article 8 III of the law).

If the two systems do not merge and have a different legal framework, the internal whistle-blower system must cover both situations.
It is this global system that is the subject of this document.

2. Anti-corruption whistle-blowing

Pursuant to Article 17 of the above-mentioned Sapin 2 Act, a code of conduct has been established, defining and illustrating the different types of behaviour to be prohibited as likely to be considered acts of corruption or influence peddling.

This code has been “integrated” into the internal regulations and, as such, it has been the subject of consultation with employee representatives. It is therefore binding on all employees of the company.

If an employee becomes aware of any conduct or situation contrary to the requirements of this code of conduct, he or she may report it under the conditions specified below.

It is specified that any report of non-compliance with the code of conduct is restricted to the company's employees only.

It is also specified that no anonymous alerts or reports will be taken into account.

3. Blowing the whistle on possible crimes and misdemeanours

3.1 The person who issued the alert: the whistle-blower

Pursuant to Articles 6 and following of the aforementioned Sapin 2 law, a whistle-blower is a natural person:

- An AMIS staff member or

• An external or occasional employee of AMIS (e.g. temporary staff member, interim manager, etc.)

who issues an alert (or blows the whistle), in a disinterested manner and in good faith on events of which he or she has personal knowledge.

3.2 The purpose of the alert

The elements that can be reported are, in part, different from breaches of the anti-corruption code of conduct.

They concern:

- a crime or misdemeanour or
- a serious and manifest breach of an international commitment duly ratified or approved by France, of a unilateral act of an international organisation taken on the basis of such an undertaking, of the law or the regulations, or
- a threat or serious harm to the public interest.

3.3 General rules on alerts

The notification of an alert shall be brought to the attention of the AMIS alert controller, in accordance with the procedures set out in paragraph II below.

In the absence of action by the controller within the time limit provided for in paragraph II-4) below, the whistle-blower may forward the alert to the judicial or administrative authority.
He or she may only make this alert public in the event of failure to be processed by the relevant judicial or administrative authority.

In the event of serious and imminent danger or in the presence of a risk of irreversible damage, the alert may, however, be brought directly to the attention of the judicial or administrative authority and, where appropriate, made public.

The AMIS controller guarantees strict confidentiality regarding
- the identity of the authors of the alert,
- the persons covered by the alert, and
- the information collected.

The priority of information processing will be based on:

1- Head of Human Resources of AMIS
2- Chief Executive Officer of AMIS
3- Secretary General of the SIFCOR Group.

Information likely to identify the whistle-blower may not be disclosed, except to judicial authorities, without the consent of the latter.

II. Processing and procedure to be followed by the AMIS controller

The following procedure must be followed as soon as an alert is issued or an alert is brought to your attention.

1. Issuing the alert

The alert can be sent by e-mail to the address: celine.bontems@amis-extrusion.fr or by depositing a letter in the mailbox provided for this purpose.

It is addressed confidentially to the AMIS company's data controller.

If this is sent by post, the envelope must be marked "*confidential - whistle-blower alert*".

To be taken into account, the alert must specify:

- The identity, position and contact details of the issuer of the alert,
- Factual elements sufficiently detailed to allow the alert to be processed,
- The identity, position and, if possible, contact details of the person(s) being reported.
- Any attachments.

It should be noted that while the alert is not anonymous, it is strictly confidential.

By way of exception, an anonymous report may be processed if the seriousness of the facts is established and the factual elements are sufficiently detailed;

In this case, the processing of the alert will have to be subject to special precautions, such as a particularly attentive prior examination, by the controller, of the appropriateness of its dissemination within the framework of the system.

2. Processing and receipt of the alert

The processing of the alert will be carried out in strict compliance with the rules applicable to the processing of personal data provided for by the CNIL and more particularly by Regulation (EU) 2016-679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data (the "General Data Protection Regulation").

The processing and any corresponding investigations are entrusted to the AMIS company's data controller and, where applicable, to an Investigation Committee, which must first be defined and set up.

- ✓ **Admissibility study:**

1. Once the alert has been received by the AMIS data controller, the latter acknowledges receipt within 48 hours (2 working days) from its author by e-mail or by post;

2. The controller shall inform the author of the alert within 15 days (working days) of its receipt, of the formal admissibility (complete file) and of the substance of the alert. If necessary, he or she will ask the person issuing the alert to complete the report in the event of missing information and will specify the time limits for communicating it. In the absence of any further information, the alert will be inoperative and cannot be processed. However, the person issuing the alert shall be entitled to issue a new alert at a later date by providing all the required information;

and informs him or her of the foreseeable and reasonable time necessary for the investigation of the case by the controller and/or the Investigation Committee

The controller may at any time request one or more experts to complete his or her analysis of the report, within the strict framework of confidentiality.

3. At the end of the period indicated by the AMIS company's controller to investigate the file, the latter shall inform the whistle-blower:

- of the action taken on the alert and the processing of the file;

- where appropriate, that a new time limit is necessary to extend the investigation of the case. He or she then specifies the foreseeable duration of this extension.

4. Upon receipt of the report and verification of its formal admissibility (complete file), the AMIS controller shall inform the person or persons concerned as soon as possible.

However, in the event that precautionary measures are necessary, in particular to prevent the destruction of evidence relating to the alert, informing such person or persons shall intervene after the adoption of such measures.

- This information specifies:

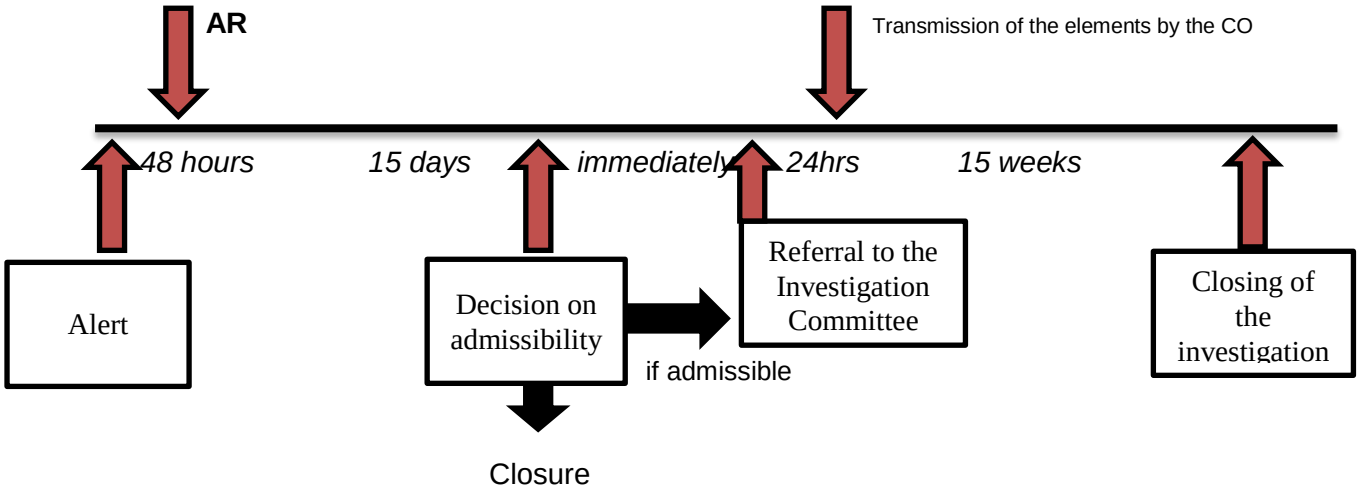
    - The person in charge of the system and his or her contact details,
    - The facts that are alleged,
    - If applicable, any recipient services of the alert,
    - The procedures for exercising his or her rights of access and rectification.

5. In order to decide whether an investigation should be initiated, the controller must first check the conditions of admissibility of the alert he or she has received.

To this end, the controller must, while remaining objective:

- examine the admissibility of the alert within a specified period of time: 15 days maximum from the receipt of the alert by the recipient;

- monitor the processing of the alert by completing Appendix 1 of the procedure, and record it on a computer or in a register dedicated to the processing of alerts with restricted access and ensure that it is kept confidential at all times.



Obligation of confidentiality:

The law imposes an enhanced confidentiality obligation on the recipients of alerts, members of the Investigation Committee and, more generally, on any person who is involved in the processing of the alert.

Respect for this confidentiality is strictly assessed, in particular with regard to the identity of the whistle-blower and the persons targeted in the alert.

No disclosure of information to persons other than those mentioned in this Article 2 will be allowed.

Important: at no time can the person targeted by the alert obtain information concerning the identity of the whistle-blower.

Any breach of this obligation will result in disciplinary and legal action.

In the event of the controller's inaction or absence, the internal auditor (AMIS Administrative and Financial Officer) shall act as deputy.

- ✓ **Decision of the controller on the follow-up to the alert**

Following the preliminary screening, the controller may:

1. Either decide to close the alert:

- He or she shall forward Appendix 1 to the Investigation Committee for information within 24 hours of the closing date. He or she only transmits his or her notes and not all the information provided by the whistle-blowing party, including information enabling the issuer to be identified.

- He or she shall inform in writing:

    - the whistle-blower of the closure of the alert and that he/she retains the possibility of referring the matter to the administrative and judicial authorities;

    - the persons targeted in the alert of the closure of the alert,

- He or she shall immediately destroy all the elements of the file making it possible to identify the author of the alert, the persons targeted by the alert and the facts.

The Investigation Committee archives the report received after anonymisation. Archiving is carried out on a dedicated computer tool with restricted access.

2. Or decide to refer the matter to the Investigation Committee to investigate the facts:

• He or she sends a report to the Investigation Committee with all the information provided by the alerting party within 24 hours of the decision to refer the matter to it.

• He or she informs the whistle-blower in writing of the referral to the Investigation Committee and informs him/her that his/her report will be processed.

III. Investigations by the AMIS Investigation Committee:

- ✓ **Conditions of appointment of the Investigation Committee:**

The Investigation Committee is composed of:

- The AMIS Data Controller (DHR)
- The Administrative and Financial Manager of AMIS
- The Chief Executive Officer of AMIS

In the event of the inaction or absence of one of the members of the Investigation Committee, the substitution is organised by a deputy appointed from each of the entities concerned (DHR, employees' representatives and Admin & Finance).

- ✓ **Investigations:**

The Investigation Committee must investigate the facts transmitted to it within 15 weeks of its referral.

The Investigation Committee ensures the follow-up of the investigation.

During the investigation, the Investigation Committee may:

- bring in other persons considered legitimate to investigate the facts, reminding them of the fundamental principles to be respected at all stages of this procedure (including by having them sign an enhanced confidentiality obligation),

- recommend immediate/corrective actions to those empowered to implement these actions,

✓ **Decision of the Investigation Committee**

Following the investigation, the Investigation Committee must close the investigation:

1. Either the Investigation Committee decides not to follow up on the alert:

- It informs the whistle-blower and the persons concerned in the alert in writing of the closure of the alert - no action is taken on the alert,

- It shall immediately destroy all the elements of the file making it possible to identify the author of the alert, the persons targeted by the alert and the facts.

The Investigation Committee archives after anonymisation the report received from the addressee at the time of its referral. Archiving is carried out on a dedicated computer tool with restricted access.

2. Or the Investigation Committee decides that the investigation has been successful:

It shall inform the whistle-blower and the persons concerned in the alert in writing of the closure of the alert that the investigation has been successful.

The Investigation Committee archives all the information collected (content of the alert, report of the alert recipient, tables completed by the Committee) on a dedicated computer tool with restricted access, guaranteeing the confidentiality of the recorded information.

Where disciplinary proceedings or legal proceedings are initiated against the person accused or implicated or the author of an improper alert, the data relating to the alert shall be kept until the end of the procedure.

IV. Miscellaneous obligations

1. Data retention

Data relating to an alert considered, as soon as it is collected by the controller, as not falling within the scope of the system shall be destroyed or archived without delay after complete anonymisation. The same shall apply where the alert is not followed by disciplinary or judicial proceedings.

However, when disciplinary proceedings or legal proceedings are initiated against the defendant or the author of an abusive alert, the data relating to the alert are kept by the AMIS controller until the procedure is completed.

In this case, the data that are subject to archiving measures shall be kept, within the framework of a separate information system with restricted access, for a period not exceeding the time limits for litigation proceedings.

2. Closing the file

The person issuing the alert and the persons concerned shall be informed of the closure of the file.

3. Compliance with the rights of access and rectification

In accordance with Articles 39 and 40 of the amended Act of 6 January 1978, the person in charge of the whistle-blowing system guarantees any person identified in the whistle-blowing system the right of access to the data concerning him/her and to request, if they are inaccurate, incomplete, ambiguous or outdated, rectification or deletion.

The person who is the subject of an alert may under no circumstances obtain from the controller, on the basis of his right of access, information concerning the identity of the sender of the alert.

4. Information for employees and occasional employees

This document has been presented and has been the subject of consultation with the works council and the CHSW respectively on..... and..... (or “of the AMIS Social and Economic Committee, dated ..... ”).

This whistle-blowing procedure is brought to the attention of employees and external and occasional collaborators for whom the system is designed. To do so, this document is available on the company's intranet and for consultation in the personnel department.

*****

The AMIS controller is required to strictly respect the following measures guaranteeing the confidentiality of the person making the report, the facts subject to the report, and the persons concerned:

The automated processing of alerts is established in accordance with Regulation (EU) 2016-679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data (the "General Data Protection Regulation" or "GDPR") which entered into force on 25 May 2018.

Appendix 1: Preliminary screening - Examination of the admissibility of the alert by the Data Controller and Report

Reminder: - Deadline to inform the whistle-blower of the receipt of his or her alert: 48 hours

- Time to perform preliminary sorting: 15 days from receipt of the alert

the anonymous alert should only be processed if the facts are serious and the alert is based on detailed evidence.

Preliminary screening of alerts – Admissibility study	
Date and time of receipt of the alert	xx/xx/xxxx - xx.xx
Identity of the alert recipient	Name: First name: Position:
Conditions of the alert	***Check the relevant box(es)***
Quality of the first recipient of the alert (a checkbox must be ticked)	[ ] direct superior [ ] indirect superior [ ] Data controller (referent alert)
Author of the alert (two boxes must be ticked)	[ ] natural person [ ] employee [ ] external and occasional employee of the company [ ] Anonymous alert
All three boxes must be checked	[ ] facts revealed in a disinterested manner [ ] facts revealed in good faith the whistle-blower has personal knowledge of the information
Scope of the alert (a box must be ticked)	[ ] a breach of the Anti-Corruption Code of Conduct [ ] a crime or misdemeanour, [ ] a serious and manifest breach of the law or internal regulations, [ ] a threat or serious harm to the public interest, [ ] a serious and manifest breach of an international commitment duly ratified or approved by France, of a unilateral act of an international organisation taken on the basis of such an undertaking, of the law or the regulations, [ ] an act contrary to SIFCOR's Anti-Corruption Policy, [ ] other – (specify):
Description of the elements provided by the alert author	[ ] yes [ ] no
Description of the elements provided by the alert author	*Add a description: e.g. document type]*

Preliminary screening of alerts – Report	
Date and time of the report	
Check the corresponding box:	
Scenario 1	[ ] the alert does not meet the conditions required by law
Scenario 2	[ ] the alert meets the conditions required by law
Decision of the alert recipient on the action to be taken on the alert	[ ] The recipient decides to close the alert [ ] The recipient decides to refer the matter to the Investigation Committee to investigate the facts reported
Comments for the Investigation Committee	*[Complete if necessary]*

Appendix 2: Investigations of alerts by the Investigation and Reporting Committee

Reminder: - Deadline to complete the investigation: 15 weeks from the date of referral to the Investigation Committee by the addressee of the alert

Date and time of referral to the Committee	xx/xx/xxxx - xx.xx
Composition of the Committee	*[Specify whether and why other persons are being referred to the investigation]*
WHO?	*Who is involved or concerned?*
WHAT?	*Scope and purpose of the investigation?*
	Nature of allegations/suspicions?
	Financial and other consequences?
	Immediate actions to preserve proof and evidence?
	Potential results of the investigation (litigation, report, disciplinary action, etc.)?
WHERE?	*Number of subsidiaries/services involved?*
	French legislative environment? English? European?
WHY?	*Reason for the breach?*
	Reasons for late detection of the breach?
WHEN?	*When did the breach occur?*
	Is the breach over? Is it still ongoing? Is there a risk of it happening?
	Which financial years are affected?
Others	

Investigations - Report	
Date and time of the report	
Check the corresponding box:	
Decision of the Investigation Committee on the follow-up to the alert	[ ] The Investigation Committee closes the alert without taking any action [ ] The Investigation Committee closes the alert after a successful investigation
Comments and Recommendations of the Investigation Committee	*[Complete as appropriate - e.g., immediate/corrective actions, etc.]*