SFA GROUP

Shaking up water

PROCEDURE INTERNAL/ EXTERNAL WHISTLE-BLOWING SYSTEM

2022/EN (V19072022)

Table of contents

1. Préambule

This procedure presents the framework of the **Whistleblowing system**.

Since most countries have regulations in place applicable to whistleblowers, in particular, the European directive 2019/1937 on the protection of persons who report breaches of Union law, this procedure has been developed in collaboration with LERINS law firm based on this directive and on one of the most stringent regulation - i.e. the French regulation.

For harmonization purpose, this system is applicable in all entities of the SFA Group.

It has been validated by the SFA Group's Ethics Committee.

Each SFA entity is aware of the local regulation applicable in the field of whistleblowing and has verified the compliance of this procedure with the latter, and/or has identified any specificities that will be taken into account in the processing of any alert.

Each SFA entity has to take appropriate mesures to ensure the enforceability of this procedure against any relevant indivual who could be the author of an alert.

2. Author of the alert

This whistleblowing procedure is intended for the following **individuals** who, in the course of their professional activities, have obtained information concerning facts that have occurred or are very likely to occur in the entity concerned, and who wish to report or disclose these facts, and in particular:

» a member of the SFA Group's staff;

» a person whose employment relationship with the SFA Group has ended, where the information was obtained in the course of this relationship;

» a shareholder, partner and holder of voting rights in the entity's general meeting;

» a member of the administrative, management or supervisory body;

» a contractual partner, its subcontractor or a member of the administrative, management or supervisory body of that contractual partner or its subcontractor and their employees;

» an external and occasional staff member, including, but not limited to:

- an employee made available by a third-party company;
- a temporary worker;
- an intern or alternating worker;
- a consultant or independent service provider;
- a subcontractor.

IDENTIFICATION OF THE WHISTLEBLOWER

It is recommended that the whistleblower declares his identity (name, first name and contact details) in his/her alert in order to ensure his clear and precise identification.

The identification of the whistleblower will allow him/her to benefit from a protection regarding the consequences of the alert, as well as a better management and a faster processing of the alert.

The identity of the whistleblower, as well as all the information collected in the context of the whistleblowing, will be processed as strictly confidential.

3. Purpose of the alert

3.1 Facts included in the scope of the alert

Individuals who notice any of the facts mentioned below are invited, within the framework of our transparency policy, to report them:

1 **A crime or an offence**

»**It should be noted that crimes must be reported to the competent judicial authorities as a priority** (Examples of crimes: murder, rape, theft with violence resulting in permanent disability, etc.)

» **Examples of offences:** corruption, tax fraud, illegal taking of interest, discrimination, moral or sexual harassment, violation of the secrecy of correspondence, misuse of company assets, breach of trust, influence peddling, etc.

2 A violation or an attempt to conceal a violation

» of an international commitment regularly ratified or approved by [country of the SFA entity];

» of a unilateral act of an international organization taken on the basis of such a commitment;

» any applicable law or regulation.

3 A threat or prejudice to the general interest

» Case-by-case assessment of situations likely to threaten or harm the general interest, without a criminal offense or violation of law being involved.

» **Examples**: harm to public health, public safety or to the environment, aggressive tax optimization, serious management error, or concealment of evidence relating to any protected alerts.

3.2 Facts excluded from the scope of the alert

The scope of the whistleblowing system does not include facts, information or documents, regardless of their form or medium, the revelation or disclosure of which is prohibited by the provisions relating to::

- » national defense secrecy;
- » medical secrecy;
- » secrecy of judicial deliberations;
- » secrecy of the investigation or of the judicial inquiries;
- » attorney-client privilege.

Secrecy does not apply to facts that are clearly made public.

4. Conditions for reporting

When reporting or disclosing any of the above mentioned facts, the whistleblower must act in **good faith** and **without direct financial compensation.**

The whistleblower must not derive any benefit, financial or otherwise, from reporting	The whistleblower must not be motivated by personal grievance, animosity or intent to harm	The whistleblower must have reasonable grounds to believe that the reported misconducts are true

It is not necessary for the whistleblower to have **personal** knowledge of the facts in question when the information was obtained in the course of professional activities. The whistleblower can thus report facts that have been reported to him.

On the other hand, when the information was obtained outside the framework of professional activities, the whistleblower must have personal knowledge of the facts. The whistleblower must be the source of the information and not have received it from another person. The report must therefore concern elements of which the whistleblower is able to assess the reality himself.

If necessary, the whistleblower must provide any fact, document and/or information, whatever its form or medium, that may support his or her report.

5. Protection of the whistleblower

5.1 Strict confidentiality

The **whistleblower**, the **persons targeted** by the alert and **any third party mentioned in the alert,** as well as **all the information** collected within the framework of the whistleblowing system will be confidential, including in the case of communication to third parties when this is necessary for the sole purpose of verifying or processing the alert.

Information that could identify the whistleblower may only be disclosed with the whistleblower's consent.

By way of exception, they may however be communicated to the judicial authority, in the event that the persons responsible for collecting or processing the alerts are required to report the facts to the judicial authority. The whistleblower is then informed (with written explanations), unless this information could compromise the judicial proceedings.

» The person targeted by the alert may not, under any circumstances, obtain information concerning the identity of the whistleblower.

» Information that could identify the person targeted by the alert may only be disclosed, except to the judicial authority, once it has been established that the alert is well-founded.

» **Disclosing the aforementioned confidential material is punishable in accordance with the local regulation and/or internal rules of the entity.**

5.2 Conditions applicables to the protection of whistleblowers

The whistleblower shall benefit from the protections provided in this procedure if:

» he/she had reasonable grounds to believe that the information on breaches reported was true at the time of reporting and that such information fell within the scope of this procedure;

» he/she reported the internally in accordance with this procedure.

Where an alert or a public disclosure has been made anonymously, the whistleblower, whose identity is subsequently revealed, benefits from the same protections.

5.3 Exemption from liability for violation of a secret

The whistleblower benefits from a protection. As such, the whistleblower cannot be punished for having communicated information covered by one of the secrets protected by law, provided that he/she had reasonable grounds to believe that the reporting was necessary for revealing a breach.

The whistleblower does not incur liability in respect of the acquisition of or access to the information which is reported, provided that such acquisition or access did not constitute a self-standing criminal offence.

5.4 Prohibition of any sanction or discriminatory measure

No person may be excluded from a recruitment procedure or from access to an internship or training period in a company, no employee may be sanctioned, dismissed or be the subject of a direct or indirect discriminatory measure, particularly with regard to remuneration, incentive schemes or the distribution of shares, training, reclassification, assignment, qualification, classification, professional promotion, working hours, performance evaluation, transfer or renewal of contract, or any other retaliation measure, threats or attempts to do so, for having::

i. reported or testified, in good faith, about facts constituting an offence or a crime of which he/she became aware in the performance of his/her duties;

ii. reported or disclosed information as defined herein;

iii. suffered or refused to suffer repeated acts of psychological harassment or having, in good faith, reported or testified to such acts;

iv. suffered or refused to suffer repeated acts of sexual harassment, including, if the comments or behaviour were not repeated, or having, in good faith, testified to acts of sexual harassment or reported such acts.

Moreover, these persons benefit, in particular, from the protections mentioned in Article 5.1.

5.5 No civil or criminal liability for disclosure of information

Persons who have reported or publicly disclosed information as provided for herein (as well as facilitators[1] and individuals in contact with the whistleblower[2]), shall not be civilly liable for damages caused by their reporting or public disclosure if they had reasonable grounds to believe, at the time of reporting or public disclosure, that the reporting or public disclosure was necessary to reveal a breach.

Persons who have reported or disclosed information as provided for herein are not criminally liable.

5.6 Prohibition of retaliation measures, threats or attemps to do so

Persons who have reported or disclosed information under the conditions herein defined (as well as facilitators and individuals in contact with the whistleblower) shall not be subject to any retaliation measures, threats or attempts to take such measures.

In the event of retaliation, the above-mentioned persons shall have recourse and the other party shall have the burden of proving that its decision was duly justified.

5.7 Sanctions for hindering the transmission of an alert

Any person who hinder in any way the transmission of an alert is subject to sanctions.

[1] Facilitators include, in particular, any individual who assists a whistleblower in making a report or disclosure under the conditions herein defined.

[2] Individuals in contact with a whistleblower are those who are at risk of retaliation, threats or attempts to do so in the course of their professional activities by their employer, their client or the recipient of their services.

5.8 Vexatious proceedings

In proceedings against a whistleblower on account of the information reported or disclosed, if the action is considered to be vexatious, specific penalties are applicable to the person that brings the proceedings.

6. Procedures to be followed for issuing an alert

The reporting of an alert can be done, at the **choice of its author**, according to one of the following procedures:

Internal channel	External channel	Public disclosure
Internal reporting should be used, in particular, when the whistleblower believes that the violation can be effectively addressed through internal reporting and that there is no risk of retaliation. The alert can be brought to the attention of: - the direct or indirect supervisor ; - the employer ; - the SFA Group Ethics Committee.	The whistleblower sends an external alert, either after having made an internal alert, or directly to: - the competent authority; - to the defender of rights, who will direct the whistleblower to the appropriate authority or authorities; - the judicial authority; - to an EU institution, body or agency.	The whistleblower may make a public disclosure: - after having made an external alert, preceded or not by an internal alert, without any appropriate action having been taken in response to this alert at the end of the feedback period; - in the event of serious and imminent danger or, for information obtained in the context of his professional activities, in the event of imminent or obvious danger to the general interest; - or when referring the matter to one of the competent authorities would expose the author to a risk of retaliation or would not enable to effectively address the subject of the disclosure

7. Recipients of the internal alert

The reporting of an alert through the internal channel is brought, **at the choice of the author**, to the attention of:

- his/her manager, his/her director
- his/her HR representative
- the local CSR representative
- the SFA Group Ethics Committee
- or the referent designated by the latter (internal or external).

Thus, the author of the alert chooses to address one or the other of these persons / entities.

The SFA Group has designated the following as the referent likely to receive professional alerts: the service provider **SpeakUp** of People Intouch B.V:

Web SpeakUp : https://sfagroup.speakup.report/sfagroup
App SpeakUp : Download « SpeakUp by People Intouch »

The SpeakUp tool and its use are presented in the appendix to this procedure: *"**SpeakUp** Reporting Tool, Employee guide"*.

The members of the Ethics Committee, in charge of handling professional alerts, must have the necessary competence to handle such alerts (specific training required).

In addition, they are bound by a contractually defined obligation of reinforced confidentiality.

8. Modalities for sending the internal alert

It is possible to report the existence and/or occurrence of any of the facts restrictively listed herein, by :

» **email:**
o to the email address of the chosen recipient: his/her manager, director or HR representative or his/her CSR representative
o to the dedicated email address of the Ethics Committee **Ethics@sfagroup.com ;**

or

» using the **SpeakUp** reporting tool
Web SpeakUp : https://sfagroup.speakup.report/sfagroup
App SpeakUp : Download « SpeakUp by People Intouch »

N.B Any recipient of an alert should in turn report it to the SFA Group Ethics Committee by email or via SpeakUp.

9. Follow-up and processing of the internal alert

9.1 Acknoledgement of receipt

Following receipt of the alert, the whistleblower will receive the following information:

» an acknowledgement of receipt of the alert, within 7 days of receipt, by email to his/her professional email address or via the SpeakUp reporting tool.

» the reasonable and foreseeable time required to review the admissibility of his/her alert;

» the modalities according to which he/she will be informed of the follow-up given to his/her alert.

The feedback may in no case exceed **3 months** from the acknowledgement of receipt of the alert.

9.2 Admissibility of the alert

The Ethics Committee verifies, within a reasonable period of time, the admissibility of the alert and in particular whether:

- the person who made the alert meets the definition of a whistleblower;
- the reported facts fall within the scope of the whistleblower's report and are related to the SFA Group's business;
- the alert was issued in accordance with the legal rules specific to this system.

In order to carry out these verifications, the following may be performed:

- hearings of any SFA Group staff, agents or external or occasional collaborators;
- investigations in the information system;
- analysis of any document provided by the whistleblower.

The SFA Group may decide to use an external service provider subject to professional secrecy to carry out this verification mission, particularly if the facts prove to be particularly serious or require further investigation.

The SFA Group may decide to use an external service provider subject to professional secrecy to carry out this verification mission, particularly if the facts prove to be particularly serious or require further investigation.

External service providers who may be involved in the handling of an alert, as well as members of the Ethics Committee, are subject to a reinforced confidentiality clause[3].

9.3 Request for additional information

Upon receipt of the alert, the whistleblower may be asked for any additional information necessary for the management and processing of the alert. An email will then be sent to the whistleblower's professional email address or via the SpeakUp tool.

9.4 Investigation report

At the end of these verifications, an internal investigation **report is drawn up.** As soon as the alert is processed, the whistleblower is informed

» of the admissibility of his alert and of the appropriate actions implemented to remedy the facts denounced[4]; or

» of the closure of the file, either due to the inadmissibility of the alert or due to the lack of follow-up given to the alert. On this occasion, it is possible to refer the whistleblower to another competent service.

10. Misuse of the system

The use of this whistleblowing system in good faith by the author of an alert, even if the facts subsequently prove to be inaccurate or do not give rise to any follow-up, does not expose the author to disciplinary action.

Misuse of the whistleblowing system is punishable because of the significant damage that such an alert may cause, both to the individuals who may be targeted and to the SFA Group itself. Misuse of the system may expose its author to disciplinary sanctions as well as to legal proceedings.

11. Protection of personal data

This alert system is optional and its non-use has no consequences for the persons concerned.

[3] In the case of the use of an external service provider, the SFA Group will enter into a contract with the service provider defining the characteristics of the processing and the various obligations of the parties with respect to data protection. GDPR, art. 28.

[4] Examples: internal corrective actions, disciplinary measures against the person targeted by the alert, referral to the competent jurisdictions, recommendations of actions to the whistleblower.

11.1 Identification of the processing

The identification elements of the processing operation covered by this procedure are as follows:

Data controller	Entity concerned by the alert
Subject-matter of the processing	Management of alerts
Nature of the processing	Collection, recording, organization, structuring, storage, modification, extraction, consultation, use, communication by transmission, dissemination or any other form of provision, reconciliation or interconnection, limitation, destruction.
Legal basis of the processing	The legal basis are : - compliance with a legal obligation; - legitimate interest.
Purpose of the processing	The purposes are the reporting and processing of professional alerts.
Type of personal data	The personal data are: - identity, functions and contact details of the whistleblower; - identity, functions contact details of the persons who are the subject of an alert; - identity, functions and contact details of any third party mentioned in the alert; - identity, functions and contact details of persons involved in the collection or processing of the alert; - reported facts; - elements collected in the context of the verification of the reported facts; - report on the verification operation; - follow-up to the alert.
Category of data subjects	The data subjects are: - whistleblower; - person targeted by an alert; - any third party mentioned in the alert; - persons involved in the collection or processing of the alert; - where applicable, persons questioned in the context of verification operations

Category of data subjects	The data subjects are: - whistleblower; - person targeted by an alert; - any third party mentioned in the alert; - persons involved in the collection or processing of the alert; - where applicable, persons questioned in the context of verification operations
Recipients of personal data	The recipients are : - the manager, the HR representative or the local CSR representative of the whistleblower; - the referent (if applicable, an external service provider (subcontractor)); - members of the SFA Group Ethics Committee (if applicable, an external service provider (subcontractor)); - any auditors subject to confidentiality in the context of divestitures/acquisitions.

11.2 Rights of data subjects

The data controller ensures that the rights of the data subjects are respected in the context of the processing of personal data that it implements for the management of professional alerts.

11.2.1 Right of access to personal data

Any person whose personal data are or have been processed in the context of a professional alert (whistleblower, presumed victims of the facts, persons targeted by the alert, person mentioned in the alert, witnesses and persons heard during the investigation, etc.), has the right to access them[5].

The exercise of this right must not allow the person exercising it to have access to personal data relating to other natural persons. This limitation is specific to the rules relating to the protection of personal data and does not prevent the application, where applicable, of the rules of procedural law, fundamental freedoms (and in particular the adversarial principle), etc.

11.2.2 Right to rectification of personal data

The right of rectification must be assessed in the light of the purpose of the processing[6].

[5] RGPD, art. 15.

[6] RGPD, art. 18.

In the case of whistleblowing systems, it must not allow the retroactive modification of the elements contained in the alert or collected during its investigation.

Its exercise, when admitted, must not lead to the impossibility of reconstructing the chronology of possible changes in important elements of the investigation.

Therefore, this right can only be exercised to rectify factual data, the material accuracy of which can be verified by the data controller with evidence, without deleting or replacing the data, even if incorrect, initially collected.

11.2.3 Right to erasure of personal data

The data subject may request the erasure of his/her personal data when one of the following grounds applies:

- the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
- where applicable, the data subject objects to the processing of his or her personal data where there are no compelling legitimate grounds for the processing;
- the processing of personal data does not comply with the provisions of the applicable regulations on the protection of personal data[7].

The right to erasure of personal data is not a general right and can only be exercised if one of the above grounds applies.

11.2.4 Right to to restriction of processing of personal data

The data subject shall have the right to obtain from the controller the restriction of processing where any of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject objects to the erasure of the data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing but they are required by the data subject for the establishment, exercise or defense of legal claims[8].

11.2.5 Right to object to the processing of personal data

In accordance with Article 21 of the GDPR, the right to object cannot be exercised for processing necessary to comply with a legal obligation to which the controller is subject[9].

Therefore, it cannot be exercised with regard to processing operations set up by the data controller that meet the conditions defined in this procedure.

[7] RGPD, art. 17

[8] RGPD, art. 18.

11.3 How to exercise your rights

Requests to exercise the rights of data subjects shall be made:

» to the following email address: **Ethics@sfagroup.com**

11.4 Retention of personal data

The retention periods applicable to data collected under the whistleblowing system are as follows:

- when the alert does not fall within the scope of the system, the data will be immediately destroyed or anonymized;

- when no action[10] is taken on an alert falling within the scope of the system, the data will be destroyed or archived, after being anonymized, within two (2) months of the closing of the admissibility or verification operations;

- when the alert is followed by a disciplinary or judicial procedure against a defendant or the author of an abusive alert, the data will be destroyed at the end of the procedure or after the limitation period for appeals against the decision.

With the exception of cases where no action is taken on the alert, the data controller may keep the data collected in the form of an intermediate archive for the purpose of protecting the whistleblower or to establish continuing violations. This retention period is strictly limited to the purposes pursued, determined in advance and made known to the data subjects.

Data may be kept longer, in intermediate storage, if the data controller is legally obliged to do so (for example, to meet accounting, social or tax obligations).

[9] RGPD, art.21.

[10] *The term "action" refers to any decision taken by the organization to draw consequences from the alert. This may include the adoption or modification of the organization's internal rules (internal regulations, ethics charter, etc.), a reorganization of the operations or services of the SFA GROUP, the imposition of a sanction or the implementation of legal action*

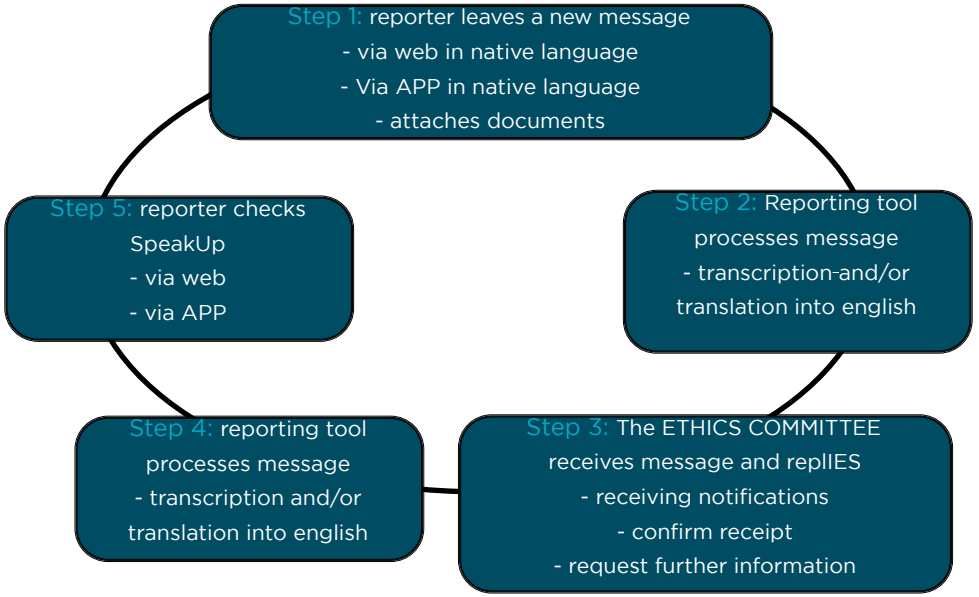
APPENDIX

Shaking up water

SPEAKUP REPORTING TOOL, EMPLOYEE GUIDE

TALE OF CONTENTS

SPEAKUP :
HOW TO LEAVE A MESSAGE



Leave a message

You can choose to leave a message through the SpeakUp® web or APP system.

Web SpeakUp: please visit « https://sfagroup.speakup.report/sfagroup »
App SpeakUp: download « SpeakUp by People Intouch »

(We advise you to write your message beforehand; this way you are sure of the information you are about to communicate and that your message is complete and relevant.)

Please have a pen ready when you leave the message. You will receive a randomly generated six-digit personal file number. It is very important that you write this down, as you will need it to read the answer from the Ethics Committee when you later re-enter the SpeakUp® system.

If you are using the SpeakUp system, you can type or simply copy and paste your message. You can also upload and attach documents to your message. When you are finished, press the "send message" button; a screen will appear with your file number and message, which you can easily print.

What happens in the meantime?

As soon as you send your message, the reporting system initiates, if necessary, the translation of the message in english.

Once the transcription and translation are complete, the exact message will be sent to the Ethics Committee.

The Ethics Committee is informed of the alert sent. It analyzes the data of the message and evaluates the conduct to be taken to answer and process it. It ensures that the whistleblower remains totally anonymous and protected. The whistleblower benefits from a criminal immunity. The Ethics Committee can also decide not to follow up the alert if it considers it inadmissible. It may also decide to call on an external service provider subject to professional secrecy to assist it in resolving the matter brought to its attention.

Consultation of the answer

An acknowledgement of receipt will be sent to you within seven days and a feedback within months on the SpeakUp system. In general, you will be able to view this answer in the same manner as you left your message, using the contact information provided above.

If you notice that you have not yet received any answer, please be assured that the message is being reviewed and a answer will be sent to you as soon as possible. It is advisable to check regularly to see if an answer has been received.

2 FREQUENTLY ASKED QUESTIONS ABOUT THE SPEAKUP SYSTEM

2.1 WHAT IS SPEAKUP?

This is a tool that allows employees (or stakeholders) to report serious misconduct while guaranteeing complete anonymity if they wish. You can make your reports either by app or through a secure website, without having to go through a human operator.

2.2 WHAT IS THE PURPOSE OF THE SPEAKUP TOOL?

The SpeakUp tool has been put in place to promote transparency in professional and commercial exchanges and to ensure that we meet our legal obligations, in particular with regard to the "European Directive on whistleblowing" protecting whistleblowers. However, the SpeakUp tool should not replace direct dialogue, as it is part of our corporate culture and we absolutely want to preserve it. This tool should be used as a last resort or because we realize that it is very difficult to talk about it.

It is also intended to be used as a way to ask questions. This tool can be used by victims or witnesses to learn about their rights anonymously when they decide to make a report.

(Our advice: see the SFA Group's reporting procedure)

2.3 HOW DOES SPEAKUP WORKS?

Website: Go to the SpeakUp web service page (via a hyperlink or by entering the URL address), select your country, enter your access code and leave your message. Within a week, you will be able to return to the Web Service and view the answer from the Ethics Committee. You will be able to submit a reply to this answer. This communication cycle can be repeated ad infinitum.

App: Access the SpeakUp application, create a confidential password and scan the QR Code of the SFA Group for SpeakUp.

2.4 WHO MANAGES SPEAKUP?

The service is managed by a third party, People Intouch, an independent Dutch company. People Intouch is responsible for processing all messages. The company was founded in 2004 and is based in Amsterdam. The SpeakUp® reporting system is already used by many renowned companies such as SNCF.

2.5 IS IT DIFFICULT TO USE THE SYSTEM?

No, you are guided every step of the way.

2.6 CAN MY IDENTITY BE DISCOVERED?

If you leave your contact details in your message, SpeakUp will pass them on; if you do not provide your contact details, SpeakUp and the SFA Group Ethics Committee will not know who you are. In addition, the company is committed to not tracing the identity of a caller and will not disclose the identity of the caller or of a witness to an accused person. Only the competent administrative authorities (justice) could be entitled to question the system in case of a serious offence.

2.7 CAN THE COMPANY TRACK MY LOGIN DATA?

No, the SpeakUp system is managed by a third party. The SFA Group has no access to login data. IP addresses will never be transmitted to the SFA Group. However, your company may track user information from your business phone or computer. Please note that you may also use a public or unidentifiable phone or computer.

2.8 WHAT ABOUT RECORDING MY MESSAGE?

Once the Ethics Committee has acknowledged receipt of the transcribed and/or translated message, the recording will be immediately erased by an external software provider.

2.9 WILL CONFIDENTIALITY EVER BE BREACHED?

Exception to the above: if the SpeakUp system receives a message in which the caller threatens violence or criminal act, the SFA Group Ethics Committee may request to retain the recording for the purpose of turning it over to the authorities. However, the connection data will never be given to the Ethics Committee.

2.10 HOW LONG WILL IT TAKE FOR MY MESSAGE TO BE FORWARDED TO THE COMPANY?

Your message, once translated if necessary, will be forwarded to the Ethics Committee within one business day.

2.11 WHO IN THE COMPANY RECEIVES MY MESSAGE?

The SFA Group Ethics Committee, located at SFA's headquarters in Paris.

The list of committee members can be found in the brochure "CSR Governing Committee of the SFA Group"

2.12 I WANT TO REMAIN ANONYMOUS, BUT I WOULD LIKE TO RECEIVE AN ANSWER, HOW CAN I DO THAT?

The SpeakUp system will provide you with a unique case number. Please be sure to write it down carefully. This case number will allow you to listen to or read the answer from the Ethics Committee when you return to the system.

2.13 WHEN CAN I GET AN ANSWER?

The Ethics Committee strives to send an acknowledgement of receipt within seven days and feedback within 90 days.

If there is no answer within a week, we advise you to enter a new message in the same file.

2.14 CAN I LEAVE A MESSAGE IN MY NATIVE LANGUAGE?

Yes, you can leave a message in your native language. Agreements are made with the SFA Group regarding language options for each country. When you leave your message, simply select one of these languages. Answers will also be communicated in your native language.

2.15 CAN I ATTACH DOCUMENTS?

Yes, the SpeakUp web service allows you to attach (electronic) documents.

When you leave a message on the phone system, you can connect to the web system using the same file number. Press the button "if you already have a file number". You can file your (electronic) documents here.

If you want to remain anonymous, make sure that your contact details are not included in the attachments or their properties.

2.16 WHAT IF I HAVE FORGOTTEN MY FILE NUMBER?

If you have lost your case number, we ask that you leave your message again with a new case number. Use the new file number for all future communication.

2.17 I DON'T KNOW WHERE TO FIND THE INFORMATION TO LEAVE A MESSAGE. WHERE CAN I FIND IT?

The information to leave a message is on page 20.

2.18 WHAT IS PERSONAL DATA? IS MY PERSONAL DATA PROTECTED BY LAW IF I LEAVE A MESSAGE THROUGH SPEAKUP?

Personal data is (in short) information that can be used to identify (directly or indirectly) a person (e.g. name, address, photo, phone number), who could be you or another person mentioned in your message. The processing of personal data by the SpeakUp system is strictly regulated (by the General Data Protection Regulation (GDPR)).

2.19 WHAT ARE MY RIGHTS IF I LEAVE A MESSAGE CONTAINING MY PERSONAL DATA THROUGH SPEAKUP?

SFA Group is required to ensure that your rights under the GDPR are respected, including: the right of access, the right of rectification, the right to erasure/to be forgotten, the right to restriction of processing, the right to data portability, the right to object and the right to lodge a complaint with the supervisory authority. SFA Group's internal policies must specify how these rights may be exercised. The SFA Group must also notify the data subject of the occurrence of an alleged "personal data breach", if it poses a high risk to the rights and freedoms of the data subject.

2.20 WHY IS MY CONSENT TO THE PROCESSING OF PERSONAL DATA NOT SOUGHT WHEN I LEAVE A MESSAGE IN THE SPEAKUP SYSTEM?

Employees, such as you, are (generally) not considered to be able to freely give, refuse or revoke your consent, as long as there is a relationship of dependence arising from the employee/employer relationship. Any personal data contained in a message that is processed by the SpeakUp system is processed on the basis that it is necessary to detect a breach that would not otherwise be detected.

SFA GROUP REPORTING PROCEDURE

1. SPEAK UP

Concerned about misconduct?

I am worried this gift is too expensive

I suspect misuse of company assets

I feel discriminated or harassed

I suspect bribes are being paid

Is this fraud ?

2. WHO CAN I TALK TO?

If possible, talk to the person involved

Talk to your manager, your managers manager or HR representative

Contact your local CSR representative

Contact the SFA Group Ethics committee under ethics@sfagroup.com

3. I CAN ALSO...

(REMAINING ANONYMOUS)

Go to **https://sfagroup.speakup.report/sfagroup** to file a report

or

Use the app «**SpeakUp by People Intouch**» and scan the QR Code to get started

REPORT IT WITH SPEAKUP

We understand it is not always easy to raise concerns about possible misconduct but we do encourage you to come forward with any concerns and speak up! Any concern will be dealt with appropriately and confidentially.

SFA GROUP
Shaking up water

SFA GROUP
Shaking up water

FOR ALL INFORMATION ON ETHICS AND COMPLIANCE OR TO REPORT AN ETHICS INCIDENT TO THE GROUP, CONTACT: ETHICS@SFAGROUP.COM

SFA GROUP
41 BIS AVENUE BOSQUET
FR - 75007 PARIS
TEL. : +33 (0)1 44 82 39 00
FAX : +33 (0)1 44 82 39 01

2022-07-19_PROCEDURE INTERNAL EXTERNAL WHISTLEBLOWING SYSTEM_EN