RED FLAG PROCEDURE

Applies from 1 April 2020

CONTENTS

INTRODUCTION

In adherence with the “Sapin II” law of 9 December 2016 regarding transparency, combating corruption and modernising business practices, ECF Group has created a procedure for preventing, detecting and fighting against corruption.

This red flag procedure aims to support ECF Group’s ethical approach and give employees an additional way to express themselves so that they can all contribute to this approach and prevent the risks associated with it.

With this in mind, ECF Group wanted to establish a single “Whistleblower” procedure for general red flags and anti-corruption warnings.

This procedure is **optional** and must be used in **exceptional** circumstances. It is not meant to replace traditional internal communication channels, depending on the applicable laws in each country.

If employees have any doubts or concerns as to the application of the law or ethical standards, they have several channels at their disposal: their line manager, the HR Department and the Group’s legal department.

This procedure is available in several languages in France and abroad, on our website www.ecfgroup.com.

SCOPE OF APPLICATION

1. Who can raise a red flag?

The Whistleblower can be:

- any employee working at one of the Group's French companies

- any of the ECF Group's external (temporary staff, service provider's employee, etc.) or temporary (temporary contract workers, apprentices, interns) employees.

The Group's subsidiaries operating in any other country than France should determine whether, in light of their national legislation, this procedure may be applied by their own employees in its current state. If the procedure needs to be adapted, this should be carried out alongside the Group's Legal Department. If the local legislation turns out to be incompatible with this procedure, a local procedure should be adopted.

The Whistleblower must have had **first-hand knowledge** of the issues they are red flagging.

The Whistleblower should act in an **objective manner** (without benefiting whatsoever).

The Whistleblower should act in **good faith** (they must not seek to cause harm to others). Please note that anyone who raises allegations they know to be false may be prosecuted according to the false accusations law (article 222-10 of the Penal Code). This person would be more likely to face disciplinary measures (see the chain of disciplinary actions specified in the internal rules or memorandum).

2. What can you red flag?

The red flag procedure allows you to highlight:

- A crime or offence
- A serious and clear violation of an international commitment regularly ratified or approved by France
- A violation of an international organisation's unilateral act taken on the basis of such a commitment
- A violation of the law or rules
- Threats or harms that seriously affect the public interest
- A breach of the Groups anti-corruption code of conduct

A breach could come under any of the following areas:

Competition rights – Fraud – Corruption – Conflict of interest – Financial crimes - Environmental damage – Harassment – Discrimination – An attack on human rights and fundamental freedoms

It excludes the following: Facts, information or documents, in whatever form or medium, covered by national defence secrets, medical secrets or secrets from a relationship between a lawyer and their client.

POINT OF CONTACT FOR RECORDING RED FLAGS

The point of contact designated by the ECF Group Senior Management for recording red flags is: The ECF Compliance Committee. This committee comprises:

- Human Resources Director
- Chief Legal Officer
- Finance Director

PROCEDURES FOR RECORDING AND DEALING WITH RED FLAGS

1. How do you report a red flag?

You can raise your red flag with your direct or indirect line manager, or directly to the Point of Contact mentioned above.

When your red flag is raised to your line manager, they must ask the person to report their red flag straight to the Point of Contact.

We recommend reporting your red flag directly to the Point of Contact, particularly if your line manager is involved.

You can raise your red flag either:

- By email to the following address:

compliance@ecfgroup.com

- By letter to the following address:

ECF Compliance Committee
1 and 3 rue René Clair
91350 GRIGNY
France

Remember that if the recipient does not take action within a reasonable time frame, the Whistleblower may then contact the legal authority, administrative authority or professional bodies. As a last resort, if one of these organisations fails to deal with the issue within three months, the red flag can be made public.

In the event of serious and imminent danger, or in light of a risk of irreversible damage, the red flag can be raised directly with the legal authority, administrative authority or professional bodies. It may be made public.

Anyone can raise their red flag with the human rights defender in order to be directed to the appropriate red flag recording organisation.

Once the red flag has been brought to the Point of Contact's attention, the Whistleblower can use the reporting form available on the website http://www.ecfgroup.com/.

This form helps provide the Point of Contact with:

- The supporting facts and information around the red flag
- Details for communicating with the Whistleblower (identity, role and contact details)

Regardless of whether the Whistleblower raises their red flag via this report form, they must **provide precise information** (facts, dates, locations, etc.).

The Whistleblower must also provide any document in any format or medium in support of the facts where possible (e.g. witness statements, text messages, emails, etc.).

2. How are the red flags dealt with?

STEP 1: Acknowledgement of receipt

When the Point of Contact receives a red flag, they immediately inform the Whistleblower in writing (email or letter) that they have received their red flag and provide them with a reasonable and foreseeable timeframe needed to assess its admissibility and the procedures according to which the Whistleblower will be kept informed of the follow-up to their red flag.

This acknowledgement of receipt does not mean the red flag is admissible.

STEP 2: Initial assessment

At the bottom of the information form provided by the Whistleblower, the Point of Contact conducts an initial assessment to determine if the red flag falls within the scope of this procedure (See scope of application 2.).

If the red flag is inadmissible, they inform the Whistleblower within the timeframe initially indicated and close the case.

If the red flag is admissible, the Point of Contact continues the procedure (see STEP 3).

STEP 3: Enquiry

In the first instance, the Point of Contact:

May make a written request (email or letter) for additional information or documents from the Whistleblower.

Informs in writing, with acknowledgement of receipt (email or letter), the people to whom the red flag refers, with reference to the entity in charge of the procedure, as well as the case against them, the departments receiving the red flag, and the ways in which they can exercise their rights and rectify the situation. A copy of this procedure will be sent alongside this information.

Takes all necessary precautionary measures to prevent the destruction of proof relating to the red flag. In this instance, information about the people to whom the red flag refers comes into play after these measures are adopted.

The Point of Contact will then proceed with the necessary investigations and checks by assessing the nature and seriousness of the case. The enquiry may be conducted either by an internal team or by specialist third parties.

The Whistleblower will only be associated with the enquiry process when the facts of the case need to be verified. The conduct of the enquiry, its content, its outcome and the resulting report are strictly confidential, even with regard to the Whistleblower.

STEP 4: Completing the assessment

Following the enquiry, the Point of Contact will draw up a confidential report that will be sent to the ECF Group's CEO for a decision on action required (corrective measures, disciplinary measures or legal action).

The Point of Contact will then inform the Whistleblower in writing of the completed assessment and the follow-up to their red flag. The people to whom the red flag refers will also be informed by writing of the assessment completion date.

PROTECTING THE WHISTLEBLOWER

1. Confidentiality

The ECF Group's early warning procedure is not anonymous. The ECF Group needs the Whistleblower's identity in order to gather the information needed to deal with the red flag and guarantee the employee's protection.

As directed by the CNIL, red flags raised in an anonymous manner cannot be dealt with unless the seriousness of the issues raised is established and the factual elements are sufficiently detailed, and only after an initial assessment by the Point of Contact to decide whether it is appropriate to deal with the red flag within the framework of this procedure.

The Point of Contact commits to dealing with the identities of those who raise red flags, the people referred to in the red flag and the information gathered with the strictest confidence.

Any third party involved in this early warning procedure must also commit to guaranteeing the confidentiality of all this information, via contractual arrangement, comply with the data retention policy (see below), and proceed to destroy or return all hand-written and digital information of a personal nature at the end of their assignment.

In this vein, IT tools used to gather and process the red flags will guarantee the strict confidentiality of information shared and the personal information of the person who shares it. It should be noted that:

- Any information that may reveal the Whistleblower's identity may only be shared with their consent, unless under legal obligation.

- Information that may reveal the identity of the person accused in a red flag may only be shared once the nature of the red flag has been deemed admissible.

Moreover, the entity in charge of dealing with the personal information gathered as part of this early warning procedure (the Compliance Committee) will take all precautions to safeguard the information, particularly by regularly updating individual usernames and passwords to ensure access to the information remains restricted.

2. Legal protection

The Whistleblower cannot be prosecuted for having raised a red flag in good faith, as long as the information they share is necessary and proportionate to the safeguarding of the interests involved, it is used in compliance with the early warning procedures defined by the law, and that the person meets the Whistleblower criteria set out in article 6 of Law no. 2016-1691 of 9 December 2016 relating to transparency, the fight against corruption and the modernisation of business practices. As an employee, the Whistleblower cannot be fired, penalised or discriminated against in any way for having raised a red flag in compliance with the red flag procedure.

3. Protection of personal data

Information gathered as part of this procedure is intended to meet the requirements of the Sapin 2 law as set out in the introduction. There is therefore a legal basis for complying with a legal obligation when dealing with this information. The information gathered will only be sent to the following recipients: people involved in the verification and processing of the red flags. As a reminder, information that may reveal the Whistleblower's identity may only be shared with their consent, unless under legal obligation. Similarly, information that may reveal the identity of the person accused in a red flag may only be shared once the nature of the red flag has been deemed admissible. Processes aimed at gathering information and dealing with red flags involve collecting information about identified or identifiable people (employees, workers, interns, etc.).

Early warning procedures should therefore be implemented in accordance with French[1] and European[2] applicable law. The accused individual must be informed when information relating to them is recorded (if necessary after the adoption of protective measures for keeping the proof safe), in order that they may ultimately exercise their right to oppose, access or modify their data.

[1] Law no. 78-17 of 6 January 1978 on Information Technology, Files and Civil Liberties

[2] EUROPEAN PARLIAMENT AND COUNCIL REGULATION (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free circulation of this data, and repealing directive 95/46/CE

As part of this procedure, ECF Group commits to only gathering and using information it deems relevant and necessary for dealing with the red flags. This may include:

- professional identity, roles and contact details of the employee who raised the red flag;

- identity, roles and contact details of the people that the red flag refers to;

- identity, roles and contact details of the people involved in recording or dealing with the red flag;

- issues raised;

- information gathered when verifying the issues raised;

- report of the verification processes;

- follow-up actions.

The red flag is only taken into account when information is formulated in an objective manner, in direct relation to the scope of the red flag procedure that the person raising it has direct knowledge of, and which is strictly necessary for the verification of the alleged facts. The wording used to describe the nature of the issues raised is a reflection of their presumed character.

Any information that doesn't fall within the scope of the procedure will not be dealt with as part of this procedure, and will be destroyed or protected without delay.

Information gathered may not be reused to pursue another objective that's incompatible with the objective of handling red flags at work.

In any event, all personal information is handled in compliance with theFrame of reference regarding how to handle personal information intended for use as part of an early warning procedure decreed by the National Commission on Computer Technology and Freedoms.

All individuals concerned have the right to access and modify their data, request its deletion or exercise their right to oppose or limit the processing of their information. To exercise these rights, the person needs to send their request to the following address: data@ecf.fr.

It should be noted that:

- If they want to exercise their right to access, the person who the red flag refers to can under no circumstances obtain any information regarding the identify of the Whistleblower.

- The person who the red flag refers to may only exercise their right to oppose if they do not wish to feature in the procedure. However, they may oppose the processing of their personal information if there has been an error, if they provide proof that this information has not been or no longer needs to be processed.

RETENTION PERIOD OF THE RED FLAG FILE

1. Regarding inadmissible red flags

If a red flag is not considered to fall within the procedure's scope of application when it is received by the Point of Contact, the related information must be immediately deleted or archived after being de-identified.

2. Regarding admissible red flags

If a red flag is not followed by disciplinary or legal proceedings, the information relating to the red flag is deleted or archived by the organisation responsible for handling red flags within two months from the completion date of the verification process.

When disciplinary or legal proceedings are carried out against the accused person or the person who raised an abusive red flag, the information relating to the red flag is retained by the organisation responsible for handling red flags until the proceedings are completed.

Information that needs to be archived is retained in a separate information system with restricted access, for a duration not exceeding the timeframe of the litigation proceedings.

ses données personnelles en cas d'erreur, en prouvant que ses données n'ont pas ou plus à être traitées.

[1] Law no. 78-17 of 6 January 1978 on Information Technology, Files and Civil Liberties

[2] EUROPEAN PARLIAMENT AND COUNCIL REGULATION (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free circulation of this data, and repealing directive 95/46/CE