

Société Foncière Lyonnaise Whistleblowing Procedure

Société Foncière Lyonnaise ("*SFL*" or the "*Company*") is required by Act 2016-1691 of 9 December 2016 on transparency, the fight against corruption and the modernisation of economic life (the "*Sapin II Act*") to set up an internal whistleblowing procedure.

This procedure (the "*Procedure*") complies with the French law on whistleblower protections (Act 2022-401 of 21 March 2022) and its enabling Decree 2022-1284 of 3 October 2022 on the procedures for collecting and processing whistleblower alerts and establishing the list of external authorities competent to receive such alerts, which came into force on 5 October 2022.

The Procedure describes:

- SFL's system for collecting and processing whistleblower alerts; and
- the extent and limits of the protection afforded to whistleblowers.

It applies to all SFL Group companies in France and to all alerts meeting the criteria set out below.

Contents

1. INTRODUCTION	3
2. WHO CAN SUBMIT AN ALERT?	4
3. WHAT CAN BE REPORTED?	4
4. WHO SHOULD BE ALERTED?.....	ERREUR ! SIGNET NON DEFINI.
5. HOW TO SUBMIT AN ALERT	6
6. HOW WILL YOUR ALERT BE DEALT WITH?	7
6.1. Admissibility of the alert	7
6.2. Information for whistleblowers about the processing of their alerts	8
6.3. Information for the persons implicated in the alert	8
6.4. Investigating the alert	9
6.5. Closing out the alert	10
7. HOW ARE YOU PROTECTED?	10
7.1. Protection against reprisals	10
7.2. Confidentiality	11
8. PERSONAL INFORMATION MANAGEMENT	11
8.1. Categories of personal information processed under the Procedure.....	12
8.2. Purposes and legal bases of personal information processing	12
8.3. Rights attached to the collection and storage of personal information	12
8.4. How personal information is processed and stored	13
8.5. Personal information storage period	13
9. INTERNAL COMMUNICATION OF THE PROCEDURE AND IMPLEMENTATION.....	14

1. Introduction

It is critically important that our business activities and practices comply with all applicable laws and regulations, international commitments (especially commitments to fight corruption, influence peddling and other probity and integrity breaches) and the values set out in SFL's Ethics Code of Conduct, in order to preserve the Company's reputation and ensure its sustainability.

It follows that any breach or suspected breach of the above rules and standards must be brought to SFL's attention immediately so that effective action can be taken without delay to resolve any resulting compliance issues.

If you are aware of facts that may fall within the scope of the Procedure as described in point 3, we strongly encourage you to report them.

However, this Procedure may not be used for any other purpose or in any other case not referred to below. Any whistleblower alerts received by SFL that concern matters outside the scope of this Procedure will be considered inadmissible in accordance with point 6.1 below.

Use of the internal whistleblowing procedure to report alerts is optional and failure to use it will not expose the whistleblower to any disciplinary measures. The internal procedure is in addition to the Company's other reporting channels (in particular, reporting to the individual's supervisor) and to existing legal procedures.

Whistleblowers may also choose to issue alerts directly to the competent authority, France's Défenseur des Droits, or to the courts or a European institution, in accordance with the procedures set out in Article 8 II of the Sapin II Act and Chapter II and the Appendix to the Decree of 3 October 2022. However, external reporting channels fall outside the scope of this Procedure.

Note that the guarantees and protection afforded to whistleblowers who submit an alert using the procedure described below do not apply to external reporting channels.

You should further note that:

- misuse of the whistleblowing system, in particular the deliberate submission of an alert in bad faith, may expose the whistleblower to disciplinary measures or prosecution;
- whistleblowers who use the system in good faith, even if the facts subsequently prove to be inaccurate or subsequent investigations do not lead to any action being taken, will not be exposed to the risk of any disciplinary measures.

2. Who can submit an alert?

In accordance with Article 8 of the Sapin II Act, the following persons may submit an internal alert:

- current SFL employees (including permanent staff, agents, temporary staff, interns, seconded employees, volunteers, etc.);
- former SFL employees;
- persons who have applied for a job with SFL, where the facts covered by the alert came to their attention during the hiring process;
- SFL shareholders and members of the administrative, management or supervisory bodies;
- external and occasional staff;
- the Company's co-contractors and their sub-contractors (i.e. their employees, managers, partners or shareholders).

Whistleblowing alerts submitted by these persons must:

- be issued in good faith and without any direct financial incentive;
- concern facts that have arisen or are very likely to arise within SFL or its subsidiaries (in its offices, on its worksites or in buildings owned by SFL);
- concern information obtained by the whistleblower in the course of their professional activities.

3. What can be reported?

The whistleblowing procedure may be used by the above persons to submit an alert concerning:

- a criminal offence or misdemeanour;
- a threat or harm to the public interest;
- a violation or an attempt to conceal a violation of an international commitment ratified or approved by France, or of a unilateral act of an international organisation taken on the basis of such a commitment, of European Union law, or of a law or regulation.

Although, in principle, SFL is not concerned by the secrets protected by Article 6 of the Sapin II Act, you should nonetheless note that, in accordance with Article 6, this Procedure does not apply to facts, information or documents in any form and on any medium whose disclosure is prohibited by the provisions dealing with:

- national security (e.g. facts relating to military intelligence),
- confidential medical information (e.g. facts revealed by the occupational physician),
- confidential court proceedings (e.g. facts revealed by a judge before a ruling is handed down),
- confidential information about a police investigation or judicial inquiry (e.g. facts revealed by a police officer concerning their investigation), or
- lawyer-client privilege (e.g. facts revealed by a lawyer concerning information provided in confidence by their client).

The Procedure also covers the collection of reports about conduct or situations that are in breach of SFL's Ethics Code of Conduct.

Situations covered by the Procedure include (but are not limited to):

❖ Breaches of probity:

- corruption, defined as behaviour by which offers, promises, gifts or perks are solicited, accepted or received in exchange for performing or not performing an act, or to obtain special favours or benefits;
- misuse of corporate assets, where an executive decides in bad faith to use company assets in a way that they know is contrary to the company's interests, for personal gain or for the benefit of another company or business in which they have a direct or indirect interest;
- favouritism, infringement of a contractor's right to freely bid for public contracts or to be treated equally in the tendering process.

❖ Breaches of employment law and violations of individual rights:

- discrimination;
- bullying, sexual harassment;
- obstruction of the work of trade unions;
- invasion of privacy, identity theft, unlawful recording or capture of personal data.

❖ Financial and accounting irregularities:

- falsification of accounting records with an impact on the company's assets or liabilities;
- concealment of financial or accounting transactions;
- preparation and reporting of financial information in a manner that does not comply with applicable accounting standards and procedures;
- money laundering;
- tax fraud.

❖ Irregular business practices:

- failure to comply with rules on the safety of property and people (worksites, asbestos, etc.)
- breaches of the building code.

4. Who should be alerted?

If the matters you want to report meet the criteria set out in points 2 and 3, you can submit your alert using the form created for this purpose.

Alerts are received and dealt with by the Ethics Officers:

- Emilie Germane, SFL's General Secretary, who has particular responsibility for alerts concerning financial and accounting irregularities, non-compliance with the rules governing the safety of property and people, breaches of probity, breaches of real estate law, stock market law or company law, as well as any breach of SFL's Ethics Code of Conduct;
- François Derrian, Human Resources Director, who has particular responsibility for alerts concerning breaches of employment law, infringements of people's rights and threats to their physical or mental health.

Alerts that do not fall within the above allocation will be dealt with by one or other of the two Ethics Officers according to their availability.

You can deviate from this allocation by asking for your alert to be dealt with by the Ethics Officer of your choice.

In practice, we recommend that you contact the Ethics Officer who, in view of their duties and the facts you are reporting, is best placed to deal with your alert impartially and to advise or support you concerning the measures to be taken.

The other recipients of the alert and the information required to verify and process it are:

- outside advisers, such as a law firm;
- where appropriate, the judicial authority or any other authority that is competent to deal with the facts that are the subject of the alert.

5. How to submit an alert

You should either:

- alert one of the Ethics Officers using the online form available on the SFL website, or
- telephone one of the Ethics Officers or leave a voice note requesting an opportunity to present your concerns during a virtual or physical meeting (whichever you prefer) to be organised within twenty working days. A report of the discussion will be drawn up and submitted to you for approval and signature.

Whilst it is acceptable for a report to be made anonymously, we encourage you to identify yourself so that the Ethics Officers can contact you if necessary to obtain any additional information they may need to ensure that your alert is admissible. In any event, the identity of any person making a report under this Procedure will be treated as strictly confidential.

In particular, data enabling the whistleblower to be identified will never be disclosed without their consent, except to the judicial authorities or in cases where this is necessary in order to check or process the alert.

Note that you have the option of remaining anonymous, provided that the facts set out in the alert appear to be proven and that the factual information is sufficiently detailed. In this case, special care will be taken over the processing of your alert and communications will continue under the conditions set out in point 6.3.

6. How will your alert be dealt with?

6.1. Admissibility of the alert

Upon receipt of an alert, its admissibility will be checked by the Ethics Officers. An alert will be considered admissible if the following conditions are met:

- the whistleblower provides evidence that he or she belongs to one of the categories of persons referred to in point 2;
- the whistleblower became aware of the facts in the course of their professional activity;
- the alert concerns breaches falling into one of the categories referred to in point 3;
- the alert does not concern any of the cases referred to in point 3 that are subject to an absolute ban on disclosure (disclosure of medical information, breach of national security, etc.);
- the alert concerns facts that have arisen or are very likely to arise within SFL or its subsidiaries;
- the report sets out the time and place of the alleged breaches, as well as the names of the persons involved, and includes a detailed description of the facts;
- supporting information, in whatever form or on whatever medium, is attached to the alert or personally handed over to the persons identified in point 4.

Only reports containing objective information, to the exclusion of any value judgement, that is strictly necessary to verify the alleged facts concerning actual or suspected irregularities or breaches in the areas mentioned in point 3 of the Procedure will be processed.

For as long as the reported facts have not been duly verified by SFL, they will simply be presumed to exist, without any conclusion being drawn from their existence.

You should include in your report only the information that you consider necessary for its processing. It should consist exclusively of factual information directly related to the subject of your alert.

6.2. Information for whistleblowers about the processing of their alerts

Upon receipt of the alert, an email will be sent to you within seven working days confirming that it has been received. However, just because the alert has been received does not mean that it is admissible.

The confirmation email will remind you that:

- misuse of the whistleblowing system (particularly the repeated submission of alerts that are clearly unfounded) may result in disciplinary action being taken against the perpetrator, as well as legal proceedings;
- the reported facts and your identity will be kept confidential at all stages of processing and, in particular, your identity will not be disclosed to the person who is the subject of the alert.

The email will also provide a reasonable estimate of the time needed to review the alert's admissibility, and will describe the procedure for informing you of the action taken in response to the alert. During the review, you may be asked for additional information.

If your alert does not meet the conditions set out in this Procedure, you will be notified in writing, stating the reasons why your alert is considered inadmissible.

Finally, within a period not exceeding three months from the date of receipt, you will be informed of the progress made in dealing with your alert, the measures planned or taken to check the veracity of the reported facts and, where appropriate, the measures planned or taken to remedy the situation.

6.3. Information for the persons implicated in the alert

The implicated person will be informed that they are the subject of the alert within one month of its submission, by registered letter sent to their personal address or by encrypted email sent to their business address, primarily to enable them to exercise their rights relating to the protection of their personal information as set out in point 8.

They will not be able to discover the identity of the whistleblower or any other information about them, or about any other persons concerned by the alert.

Transmission of the notification may be deferred, however, if there is a risk that notifying the implicated person will seriously compromise the verification and processing of the alert, by enabling them to disrupt the investigation or destroy evidence.

In this case, the person implicated in the alert will be informed as soon as these risks have been eliminated (for example, by suspending the implicated person or adopting other precautionary measures), and in any event no later than three months after the alert is received.

6.4. Investigating the alert

SFL will not draw any immediate conclusions from a simple alert. If the facts prove difficult to verify, as may be the case in particular when the alert is submitted anonymously, the alert may be considered as insufficiently substantiated for it to be passed on for processing.

The Ethics Officers are responsible for investigating the alerts they receive. During the investigation process, you may be asked to provide additional documents or explanations.

As a whistleblower, you may also be called for an interview. In this case, a record of the discussions will be drawn up, which you will be asked to approve and sign. In any event, the interview will be conducted under conditions of strict confidentiality for the whistleblower.

Depending on the scope and complexity of the alert and the nature of the facts in question, the Ethics Officer may be assisted by:

- internal experts,
- where appropriate, external advisers such as legal counsel.

In this case, if it is absolutely necessary to provide the internal or external adviser with information identifying you as the whistleblower in order to process the alert, your express consent will be sought.

The Ethics Officers will take all necessary steps to verify the authenticity, reality and materiality of the facts brought to their attention. As part of this process, they may interview various people, including the person(s) implicated in the alert; these interviews would not form part of any disciplinary proceedings.

If you submit your alert anonymously, discussions will continue using the reporting platform's chat function. When a message is sent via this platform, you will be notified by email.

In any event, the Ethics Officers will be bound by a strict obligation of confidentiality (specified in point 7.2.) and must deal with the alerts according to the highest standards of impartiality.

In order to conduct and monitor investigations with all the rigour and diligence required, the Ethics Officer will record the data relating to the alert on an internal computer network with restricted access to ensure that the process is tracked effectively without any breaches of confidentiality.

All investigations will be conducted in strict compliance with applicable legislation.

6.5. Closing out the alert

Within three months of receipt of the alert being confirmed, the whistleblower and the person(s) implicated in the alert will be informed that the verification process has been completed.

The Ethics Officer will draw up an investigation report setting out:

- the date the alert was received;
- the facts presented in the alert;
- the nature of the investigations into the alert;
- an analysis of the seriousness of the reported facts;
- the conclusions and action to be taken in response to the alert.

Based on this report, the Company may decide:

- to initiate disciplinary and/or legal proceedings, or
- to take no action in response to the alert.

In accordance with the obligation of strict confidentiality in the processing of alerts, you will not be given a full copy of the investigation report.

7. How are you protected?

7.1. Protection against reprisals

If you meet the conditions set out in points 2, 3, 4 and 5, you will benefit from the protection afforded to whistleblowers under the Sapin II Act.

In accordance with Article 10-1 of the Sapin II Act, no person, whatever their level in the chain of command, who has in good faith alerted the Company to suspected irregularities or breaches will be subject to any reprisals, threats or attempts to take such measures. Examples of prohibited measures are listed in the Act. SFL will at all times ensure the protection of whistleblowers in line with its obligations under the Act, by attaching particular importance to concealing their identity and by guaranteeing that no reprisals are taken against them.

By way of example, the prohibited measures set out in Article 10-1 of the Sapin II Act include the following:

- Suspension, exclusion, dismissal or equivalent measures;
- Demotion or refusal of promotion;
- Internal transfer, change of workplace, reduction in salary, change in working hours;
- Negative performance appraisals or work certificates;
- Imposed or administered disciplinary measures, reprimands or other sanctions, including financial penalties;
- Coercion, intimidation, harassment or ostracism;
- Discrimination and prejudicial or unfair treatment.

Article 10-1 of the Sapin II Act also stipulates that whistleblowers cannot be held liable under civil or criminal law. Subject to certain conditions being met, whistleblowers will not be held liable for the civil consequences of their actions, nor will they be exposed to the risk of criminal prosecution as a result of their alert.

In practice, this means you cannot be held legally liable for your alert if it was duly submitted in accordance with this Procedure.

In addition, Article 6-1 of the Sapin II Act extends whistleblower protections to:

- any individual or non-profit making private entity that helps a whistleblower to submit an alert or make a disclosure;
- any individual in contact with a whistleblower who may be subject to reprisals;
- any legal entity controlled by the whistleblower, or that employs the whistleblower or has business ties with the whistleblower.

7.2. Confidentiality

From the moment we receive the report until it is closed out, the information obtained, including your identity, that of the person implicated in the alert, and that of any third party mentioned in the alert, will be treated in the strictest confidence.

The information and documents used to process the alert will be stored on an internal server with restricted access, to which only the Ethics Officers have access.

Information identifying you as the whistleblower may only be disclosed with your consent, except to the judicial authorities.

Information identifying the person implicated in the alert may be disclosed only once it has been established that the alert is justified, except to the judicial authorities.

In any event, all persons who have access to the information collected when the alert is submitted will be required to treat it as strictly confidential. Article 9 of the Sapin II Act stipulates that the disclosure of information potentially leading to the identification of the whistleblower or the person implicated in the alert is punishable by two years' imprisonment and a fine of €30,000.

8. Personal information management

Implementation of the Procedure requires SFL to process personal information about all the persons that may be concerned by the alert and its processing, including the whistleblower, the person(s) implicated in the alert, and the Ethics Officers.

SFL undertakes to comply with the requirements of the EU General Data Protection Regulation 2016/679 and the French Data Protection Act 78-17 as amended, as well as with the applicable recommendations of the Commission Nationale Informatique et Libertés (CNIL).

8.1. Categories of personal information processed under the Procedure

The following categories of personal information may be processed by SFL under the Procedure, depending on your situation in relation to the alert (whistleblower, person implicated in the alert, person responsible for processing the alert):

- identification data (identity, last name, first name, age, contact details, etc.);
- professional data (job title, role, professional contact details, etc.);
- reported facts and data collected during the process to verify the facts;
- data included in alert verification and processing reports (investigations, interviews, etc.);
- data on the action taken in response to the alert (measures taken, sanctions, close-out, etc.).

The Procedure is not designed to systematically collect sensitive data (such as ethnic origin, political opinions, religious beliefs, trade union membership, medical conditions, sexual orientation, etc.). Nevertheless, if this type of data is communicated in the alert or more generally for the implementation of the Procedure, it may be collected and then processed by SFL only if this is necessary to establish, exercise or defend a legal right.

Similarly, data relating to offences, convictions or security measures may only be collected if and to the extent that this is strictly necessary for the purposes of the Procedure and in the cases provided for by the applicable law.

8.2. Purposes and legal bases of personal information processing

Depending on the nature of the alert and the measures implemented by SFL in accordance with the Procedure, the resulting processing of personal information may be based on:

- compliance with the legal obligations applicable to SFL, in particular under the Sapin II Act;
- SFL's legitimate interest in ensuring compliance with its Ethics Code of Conduct.

The purpose of these processing operations is to collect and deal with the alerts (checks, investigative measures), and to implement the resulting measures (close-out without any further action, sanctions, alerts, reports to the competent authorities, etc.).

8.3. Rights attached to the collection and storage of personal information

The persons implicated in an alert and the whistleblower have:

- a right of access to their personal information;
- the right to rectification of their personal information, in accordance with Article 16 of the GDPR;

- the right to erasure of personal information (right to be forgotten), in accordance with Article 17 of the GDPR;
- the right to restriction of processing, in accordance with Article 18 of the GDPR;
- the right to object to processing, in accordance with Article 21 of the GDPR.

In any event, data enabling the whistleblower to be identified, directly or indirectly, will not be disclosed to the person implicated in the alert as a result of these rights being exercised.

These rights may be exercised by any person concerned by contacting the Ethics Officers designated in point 4, by telephone or by email:

- Emilie Germane: e.germane@fonciere-lyonnaise.com, 00 33 (0)1 42 97 00 43
- François Derrian: f.derrian@fonciere-lyonnaise.com, 00 33 (0)1 42 97 00 85.

The person concerned may be asked to provide documents needed to verify their identity or to clarify the rights that are being exercised.

The person concerned will also have the right to lodge a complaint with the competent data protection authority, such as the CNIL in France, regarding the processing of their personal information.

8.4. How personal information is processed and stored

Restricted, secure access to the alert files guarantees the strict confidentiality of your identity, the facts that are the subject of the alert and the identity of the persons implicated in the alert, including in the event of communication to third parties where this is necessary for the sole purpose of verifying or processing the alert.

These files, containing all the information, documents and reports collected or prepared in connection with the processing of alerts, are stored on the restricted-access internal computer network used exclusively for the processing of alerts in accordance with this Procedure.

Finally, all persons involved in the procedure for collecting whistleblower reports are required to sign a specific confidentiality agreement.

8.5. Personal information storage period

As a general rule, the data collected and processed pursuant to this Procedure is kept for the period necessary to achieve the Procedure's purpose.

More specifically, unless otherwise provided by the applicable laws or regulations or if SFL is legally required to retain the data for a longer period:

- data which does not fall within the scope of the Procedure or which relates to alerts deemed inadmissible or which is clearly irrelevant to their processing will be destroyed or rendered anonymous without delay;
- data processed in connection with an alert which is not acted upon will be destroyed or

- anonymised within a maximum of two months from the end of the checks;
- if the alert gives rise to disciplinary or legal proceedings, the related information and processing data will be kept until the end of the proceedings or until the statute of limitations runs out;
 - if the alert leads to action being taken, the related data may be kept in interim storage (with restricted access) until the applicable statutes of limitation run out, for the ongoing protection of the whistleblower or to establish the offences concerned by the alert.

Strictly anonymised data may be kept for a longer period, in particular for statistical purposes or to comply with legal obligations.

9. Internal communication of the Procedure and implementation

This Procedure is applicable from 1 September 2023.

Prior to this date, it was submitted to the employee representative bodies for their opinion, then communicated by email to all employees and posted on the SFL website.

Lastly, whistleblowers may also submit an external alert in accordance with Article 8 II of the Sapin II Act and Chapter II of the Decree of 3 October 2022, either after having submitted an internal alert or directly.