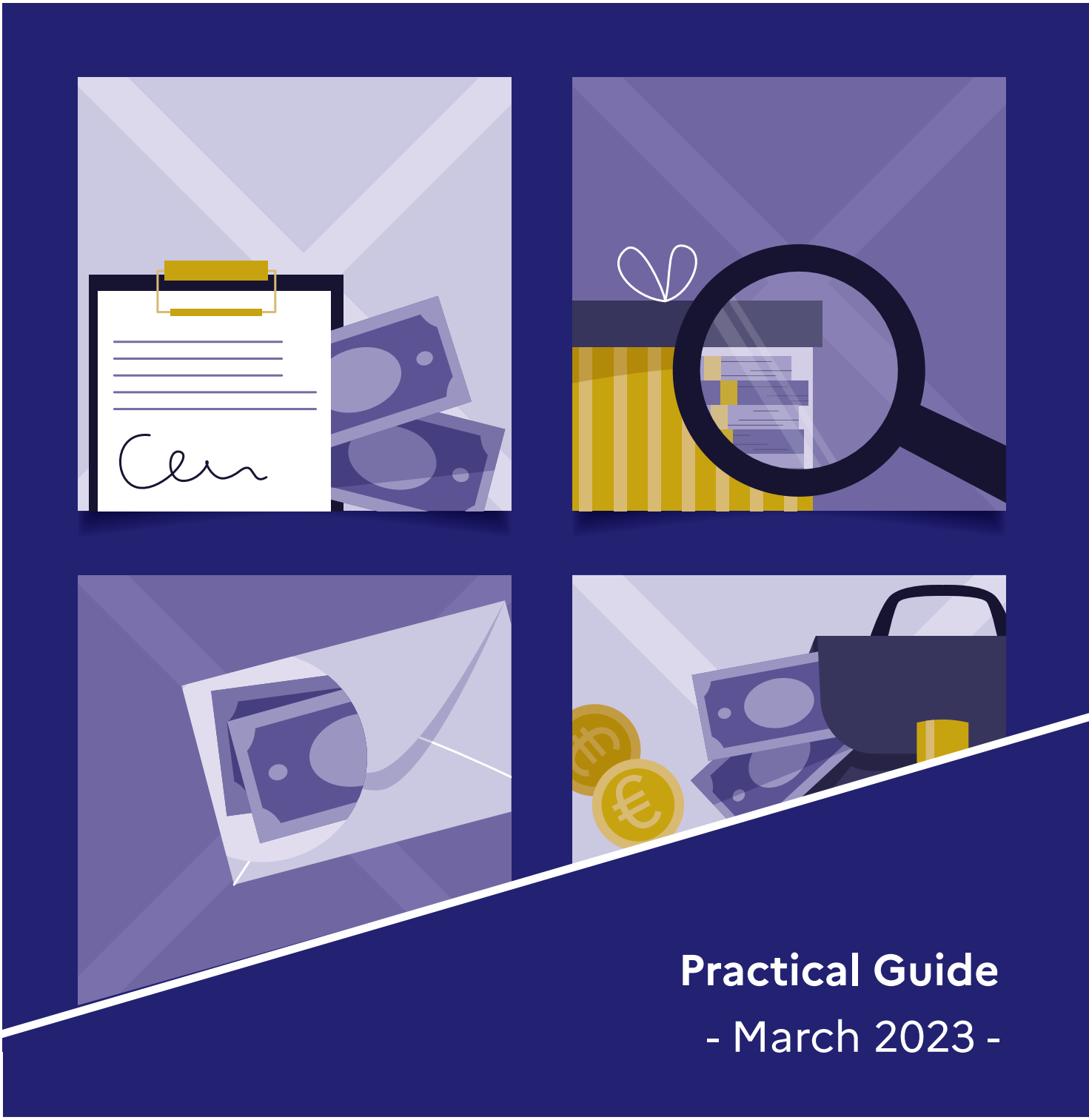
GOUVERNEMENT

Liberté
Égalité
Fraternité

INTERNAL ANTI-CORRUPTION INVESTIGATIONS



Practical Guide

- March 2023 -

AFA
Agence Française Anticorruption

French National Financial Prosecutor's Office

FOREWORD

Anti-corruption action is traditionally based on the trinity of prevention, detection and enforcement. As such, it calls for concerted and coordinated action by the different institutions tasked with combating corruption. It is in this spirit that the French Anti-Corruption Agency (AFA) and the National Financial Prosecutor's Office (PNF) signed a cooperation agreement on 28 March 2018.

This agreement focuses on AFA control disclosure procedures and notifications pursuant to Article 40 of the Code of Criminal Procedure, the terms of judicial public interest agreement ("convention judiciaire d'intérêt public", CJIP) implementation and court-ordered compliance program obligation, and training and information actions to improve awareness of corruption and related offences.[1]

Cooperation between the AFA and the PNF takes the form of joint publications to strengthen the culture of integrity among economic actors and improve their ownership of the relevant legal framework. The AFA and the PNF have therefore developed this practical guide on internal anti-corruption investigations in business as part of this process to round out the French anti-corruption policy framework.

Internal investigations are no stranger to the business world as they are regularly conducted in labour matters, in particular prior to possible disciplinary sanctions and including for potential criminal charges. However, businesses have stepped up the professionalism of their whistleblower report handling practices, which can include internal investigations, further to the entry into force of the Transparency, Anti-Corruption and Economic Modernisation Act 2016-1691 of 9 December 2016 (known as the Sapin II Act), Decree 2017-564 of 19 April 2017 on whistleblower report reception procedures, the French Data Protection Authority (CNIL) standards of 6 July 2023 on personal data processing for professional whistleblowing systems and, more recently, Act 2022-401 of 21 March 2022 on improving whistleblower protection, known as the Waserman Act, and implementing Decree 2022-1284 of 3 October 2022. Negotiated justice, introduced into French legislation by the Sapin II Act provisions on judicial public interest agreement and rolled out by extra-territorial activity of foreign prosecution authorities to counter corruption, has also contributed to the development of this practice.

Internal investigations play a full part in increasing the effectiveness of internal whistleblowing measures in businesses, improving the quality of the anti-corruption compliance program as a whole and, where relevant, enabling the implementation of a negotiated criminal justice response.

Accessible on the AFA and PNF websites, this guide has been produced to help businesses conduct internal anti-corruption investigations in accordance with individual rights and freedoms. It describes the internal anti-corruption investigation triggers, how to conduct an internal investigation and action to be taken following an internal investigation.

1 Corruption offences cover: bribery and influence peddling at both national and transnational levels, favouritism, misappropriation of public funds, unlawful taking of interest and extortion by public officials.

It presents the circumstances that can justify an internal investigation alongside watch-points for businesses and a set of recommended good practices. Although this guide only covers internal investigations related to anti-corruption matters, some good practices can be usefully considered to handle whistleblower reports within the broader scope of Article 6 of the Sapin II Act, as amended by the Waserman Act, especially if the organisation has decided to set up a single technical platform.[2]

Charles Duchaine
Director, French Anti-Corruption Agency

Jean-François Bohnert
Financial Public Prosecutor

2 AFA, Guidelines of 12 January 2021, Official Journal of the French Republic (JORF), § 253, p. 32.

CONTENT

INTRODUCTION

The internal investigation is a sound management reflex for a business and its management to have when potential breaches of the anti-corruption code of conduct or evidence of what might constitute bribery or influence peddling, at national or transnational level (hereinafter referred to as "corruption"), come to their attention. The purpose of the internal investigation is to confirm or dismiss these suspicions so that management can consider their implications and make appropriate decisions in the best interests of the business.

The internal anti-corruption investigation is therefore one of the possible steps to be taken in response to the internal whistleblower report set by Article 17 of the Sapin II Act and is therefore an integral part of the anti-corruption program.[3] The internal anti-corruption investigation is also an appropriate response in the event of a disclosure or whistleblowing by a third-party. Any cross-border element of the investigation should lead businesses to consider possible implications in view of the national or foreign legislation applicable.

An internal anti-corruption investigation refers to all the investigations conducted within an organisation at its own initiative to objectively assess: (i) potential breaches of the anti-corruption code of conduct for businesses subject to Article 17 of the Sapin II Act, (ii) non-compliance with the company's procedures to prevent and detect such breaches, and (iii) indications of acts committed that might constitute corruption.

This practical guide has been produced for the following purposes:

- Support organisations with the design and deployment of their internal investigations system in light of the upsurge in internal investigations driven by anti-corruption whistleblower reports and the development of judicial public interest agreements;
- Draw businesses' attention to the most strategic and sensitive points of the internal anti-corruption investigation, especially regarding respect of individual rights and freedoms.

As a supplement to the AFA Guidelines published in the French Official Journal No. 0010 of 12 January 2021, this guide is not binding and creates no legal obligations.

It is designed mainly, but not exclusively, for private companies and public establishments of an industrial and commercial nature (EPICs) with more than 500 employees and turnover in excess of €100 million that are subject to Article 17 of the Sapin II Act, which requires them to set up "an internal whistleblowing system for receiving reports […] about instances of conduct or situations that violate the company's code of conduct."[4]

3 AFA, Guidelines of 12 January 2021, JORF, § 266-§ 277, pp. 33-34.
4 Sapin II Act, Article 17 (II, 2).

Smaller businesses that voluntarily undertake to implement an anti-corruption program could make use of all or part of the recommendations in this guide. They could also consult the other guides published by the AFA.

SPECIFICS ON CRIMINAL INVESTIGATIONS

Criminal investigations are conducted under the supervision of prosecutors or investigating magistrates who are entirely impartial and consider both incriminating and exculpatory evidences. Investigations are conducted by trained, specialised investigators who are tasked with finding evidence of the allegations and identifying the perpetrators. Investigative work most likely to constitute a violation of rights and freedoms is strictly regulated and, in certain cases, can immediately be challenged before the relevant court.

At the end of the criminal investigation, the magistrates are responsible for deciding whether to issue a criminal indictment and prosecute or to dismiss the charges where no clear case can be established. Aside from a few rare exceptions, only a magistrate can refer a case to a criminal court.

The charges arising from a criminal investigation are tried by adversarial proceedings and the court ruling may be appealed.

The court is in no way bound by the conclusions of an internal investigation, which is neither of the same nature nor with the same purpose as a criminal investigation. An internal investigation conducted under the employer's disciplinary authority is not governed by the Code of Criminal Procedure, unlike a criminal investigation.

When a court is informed of a suspected criminal offence, it conducts in-depth investigations to gather evidences that may or may not include elements gathered by an internal investigation.

This guide describes the internal anti-corruption investigation triggers, outlines its watch-points and presents the actions to be taken following such an investigation.

1. OPENING AN INTERNAL ANTI-CORRUPTION INVESTIGATION

Triggers for opening internal anti-corruption investigation may be internal (1.1) or external (1.2.) to the organisation.

1.1. Internal events

1.1.1. Reception of a whistleblower report

An internal whistleblower report, generally from a member of staff, can justify triggering an internal investigation. Internal whistleblower reports may come from:

- The **internal anti-corruption whistleblowing system** set by Article 17 (II) of the Sapin II Act and detailed by the AFA Guidelines.[5] It is implemented by companies required to do so in order to receive whistleblower reports from their staff about instances of conducts or situations that violate the company's anti-corruption code of conduct.
- The **whistleblower report reception system** notably for crimes and offences, set up in accordance with Article 8 of the Sapin II Act amended by the Waserman Act by private sector entities with at least 50 employees to receive whistleblower reports from:
  - > Staff members, including those no longer working for the company, when the information was obtained in the course of their work for the company;
  - > Members of the board of directors, management body or supervisory body;
  - > Shareholders, partners and individuals with voting rights at the annual general meeting.

1.1.2. Action following an internal control or internal audit

The corruption prevention and detection system provided for by Article 17 (II) of the Sapin II Act requires the implementation of an internal monitoring and evaluation system which can be part of a broader internal control and audit system[6] and usefully structured around three lines of defence.[7]

As explained by the AFA guidelines, one of the objectives of these controls is "detecting any [potential] corruption."[8]

5 AFA, Guidelines of 12 January 2021, JORF, § 251-284, pp. 32-35.
6 Ibid., § 317, p. 40.
7 Ibid., § 319, p. 40.
8 Ibid., § 318, p. 40.

Substantiated and documented reports are generally drawn up on these controls by the compliance or internal control departments (second line of defence) and the internal audit department (third line of defence). In the event that they find suspicions of corruption or failure to comply with procedures to prevent and detect corruption, internal control or internal audit reports may serve as grounds to open an internal investigation.

Senior management[9] or qualified persons appointed by senior management[10] are responsible for deciding whether these reports justify opening an internal investigation. Nevertheless, if the internal control or audit activities find evidence of criminal offences even before the launch of an internal investigation, senior management is advised to notify the judicial authorities as soon as possible. It is actually best practice for the organisation to notify the judicial authorities of any serious suspicion of corruption as soon as possible and to take steps to preserve chain of custody where there is a risk of loss of integrity of evidence. In addition, the company's notification initiative may be taken into consideration by the public prosecutor when deciding whether to prosecute or to resort to an alternative to prosecution.

1.2. External events

Internal investigations can be launched: following a whistleblower report issued by a third party external to the organisation (1.2.1.); as part of an investigation opened by a French prosecution authority (1.2.2.); or following a request for information from a foreign authority (1.2.3.). They can also be opened following an external audit or control (1.2.4.).

1.2.1. Action following a whistleblower report by a third party

If the company has opted to set up a single technical platform to receive whistleblower reports in accordance with AFA guidelines,[11] it is legally bound since 2016 to extend the possibility of submitting a whistleblower report not only to company members but also to external and casual[12] collaborators[13] under Article 8 of the Sapin II Act. In addition, the Waserman Act demands that companies extend access to their whistleblowing channel to the following third parties:

- Co-contractors, their sub-contractors and, in the case of legal entities, members of its co-contractors and sub-contractors' boards of directors, management bodies or supervisory bodies and their members;
- Persons who have applied for a job in the company, when the information was obtained during the application process.

9 AFA, Guidelines of 12 January 2021, JORF, § 324, p. 40 and § 93, pp. 12-13 for a definition of senior management.
10 Generally by a duly official delegation of authority.
11 AFA, Guidelines of 12 January 2021, JORF, § 253, p. 32.
12 Consultants, for example.
13 Such as temporary staff and interns.

An internal investigation can consequently be opened following a whistleblower report made by a third party external to the organisation, especially since certain businesses choose to further extend their whistleblowing system to other third parties (competitive bidders, for example).

In the event of a whistleblower report by a third-party, and subject to the advisability of immediate referral to the judicial authorities, it is in the company's best interest to launch an internal investigation without delay to ascertain the facts of the case since the business has no control over whether the third party chooses to disclose this information more widely, if not notify the prosecution authorities. In the particular case of a whistleblower report made by a customer or a supplier, the business should also avert any negative repercussions, which could extend to a termination of contract[14] which, if the contract provides for this possibility, could be decided on by the whistleblowing third party.

In the event of a disclosure of information by the press, the company may wish to adopt an external public relations strategy to protect its reputation. A press release announcing the launch of an internal investigation could clearly state that the business is fully aware of the gravity of the allegations brought against it, its management or its staff.

The organisation can thus show that it intends to respond to the whistleblower report in an organized manner in accordance with its values, by first checking the facts of the case before, if evidence is found, acknowledging or not any transgression and taking the corrective actions it deems useful to mitigate the repercussions of the misconduct.

1.2.2. Opening of an investigation by a French prosecuting authority

When an organisation learns it is the subject of a criminal investigation,[15] it may, directly or through its lawyers, inform the judicial authority in charge of the investigation – the financial public prosecutor ("PRF") in most cases – of its willingness to cooperate with the inquiries, in particular by conducting an internal investigation.

This cooperative approach, initiated by the company without delay, enables the judicial authority to evaluate and assess, depending on the circumstances and particularities of the case, the risks of interference or benefits of the inquiries of an internal investigation by the company.

In this event, an early exchange ensures that any internal investigation is properly coordinated with the criminal investigation inquiries, since the private initiative can make a substantial contribution to improving the effectiveness of the judicial authority's action by uncovering covert situations or preserving essential evidence required to establish all responsibilities.

14 French Supreme Court of Appeal Commercial Division, 16 November 2022, Appeal No. 21-18.491.

15 This can be triggered by the option of direct referral by the whistleblower to the judicial or administrative authorities as now provided for by the Article 8 (II) of the Sapin II Act.

Contact made with the judicial authority as far upstream as possible should make it possible to achieve this joint goal without prejudice to investigation secrecy. To this end, the judicial authority should be contacted as soon as evidence of an offence emerges. However, awaiting the completion of the internal investigation and disclosure of its conclusions, a key procedure for deciding whether or not to take disciplinary action, can, in certain situations, prove detrimental to the criminal investigation's gathering of evidence. This could be the case, for example, where there is a risk of dissipation of material evidence, loss of witnesses or pressure on witnesses.

1.2.3. Request for information from a foreign authority

The organisation may directly receive information requests from foreign authorities. These requests can be made in various circumstances (judicial, administrative or agreements negotiated with businesses). When receiving a request, the company might be inclined to decide to open an internal investigation to assess in context the allegations that led to the request.

However, it is important for businesses to observe the utmost vigilance, since two scenarios are likely to arise:

- The request is made directly by a foreign judicial authority or another foreign authority: pursuant to Decree 2022-207 of 18 February 2022, the company is required to promptly contact the Economic Strategic Intelligence and Security Department (SISSE)[16] in its capacity as the one-stop centre for the enforcement of Act 68-678 of 26 July 1968 on the disclosure of economic, commercial, industrial, financial and technical documents and information to foreign individuals or entities, since only the French judicial or administrative authority can be its correspondent for the execution of international assistance requests on national soil;
- The foreign request concerns the transmission of documents or information whose disclosure is prohibited by Article 1 of Act 68-678 of 26 July 1968. The legal entity therefore also needs to immediately inform SISSE to benefit from assistance and support.[17]

In any event, and especially when a reasonable presumption of an offence has been objectively ascertained, the proper course of action is to contact the judicial authority, whether immediately upon receipt of the request and before the launch of any internal investigation, or following its launch.

16 Useful contact: loi.deblocage@finances.gouv.fr
17 Companies could usefully consult the SISSE-Afep-Medef Guide for businesses to identify the sensitive data referred to in Article 1 of what is known as the blocking or referral statute.

1.2.4. Action following an external audit or control

An internal investigation may be opened following the discovery of misstatements anomalies by an external audit. For example, this could be an acquisition audit,[18] an audit of a partner or the annual certification of financial statements for companies subject to this requirement or those that voluntarily submit to it. In the case of the certification of financial statements, auditors are bound by professional practice standards (including NEP-240) to consider the possibility of fraud in their work.[19] Auditors have to identify and assess the risk of material misstatements in the accounts, defined as one or more inaccurate, inadequate or omitted accounting or financial entries that could influence the judgement of the user of that information. Such material misstatements may be due to error or fraud, which differs from error in terms of its intentional nature. Although the purpose of due diligence by statutory auditors in their certification work is not to detect corruption, it may reveal accounting procedures designed to conceal corrupt conducts (unjustified or unwarranted transactions), provided that the irregularities in question have a significant impact on the accounts.

In addition, statutory auditors are bound by the Commercial Code to inform the public prosecutor of any offences found in the course of their diligence, failing which they risk a prison sentence and a fine.[20] The Commercial Code also requires them to report to "the next annual general meeting or meeting of the relevant body of the irregularities and inaccuracies found in the course of their work."[21]

An internal investigation may also be launched on the grounds of misstatements found during a control conducted by a regulatory authority (French Financial Market Authority (AMF), Prudential Supervision and Resolution Authority (ACPR), High Council of Auditors (H3C), etc.), an administration (tax, customs, etc.) or a private body tasked with a public service mission (e.g. Union for the Collection of Social Security and Family Allowance Contributions (URSSAF)). Some of these authorities are subject to the provisions of Article 40 para. 2 of the Code of Criminal Procedure, which requires them to immediately notify the public prosecutor[22] of any crimes or offences of which they become aware when performing their diligence. Although the detection of corruption is not the primary purpose of the controls conducted by these entities, they sometimes focus on arrangements that can be used to prevent and detect offences underlying corruption (forgery, breach of trust and misuse of corporate assets) or following corruption (concealment of the proceeds of corruption, money laundering, etc.) and which reveal attempts to conceal unlawful conduct.

18 AFA, Practical Guide on Anti-Corruption Due Diligence for Mergers and Acquisitions of 12 March 2021.
19 French Institute of Auditors (CNCC), NEP-240. Prise en considération de la possibilité de fraudes lors de l'audit des comptes.
20 Commercial Code, Article L.820-7.
21 Commercial Code, Article L.823-12.
22 Code of Criminal Procedure, Article 40.

Lastly, the decision to open an internal investigation can sometimes be justified by the existence of irregularities revealed by an audit at the initiative of the AFA. The nature of this audit is such that it can bring to light procedural weaknesses that could be conducive to corruption or incidentally lead to the discovery of irregularities that could be considered as evidences of an offence. This audit may have been conducted following a whistleblower report received by the AFA, the competent external authority referred to in Article 9 and the appendix of Decree 2022-1284 of 3 October 2022 implementing Article 8 (II) of the Sapin II Act, amended by Act 2022-401 of 21 March 2022.

2. CRITICAL ASPECTS IN INTERNAL ANTI-CORRUPTION INVESTIGATIONS

The business that conducts an internal anti-corruption investigation must ensure that the procedure complies with legal requirements to be able to take disciplinary and legal actions if necessary.

In this regard, it is recommended to define and formalize an internal investigation procedure in advance (2.1.) and to pay particular attention to the choice of investigation participants (2.2.) and how the investigation is conducted (2.3.).

2.1. Define and formalize an internal investigation procedure in advance

It is recommended to formalize an internal investigation procedure before conducting one.[23] An official procedure enables the organisation to achieve a number of key objectives:

- Organize the evidence gathering and storage procedures to guarantee its integrity and admissibility and protect it from any alteration, in particular with a view to disciplinary and/or legal proceedings;
- Guarantee compliance with the confidentiality requirements in accordance with Article 9 of the Sapin II Act regarding the whistleblower, the persons implicated by the whistleblower report, any third party mentioned in the report and the information gathered by all whistleblower report recipients;
- Guarantee the conditions for an investigation compliant with the rights of implicated staff and witnesses, including the rights of defence and the rights to privacy and personal data protection. In this respect, it is reminded that employers are bound to inform and consult the Social and Economic Committee (CSE)[24] regarding all the means of investigation and control of staff activities that could be used in an internal investigation;
- Optimize investigation lead-times by means of a procedure that defines in advance the objectives, participants, governance, investigation resources available, procedure for determining any further action to be taken following the investigation, and the record keeping and archiving system. In the case of a multistep investigation, any applicable timeframes need to be stipulated for each step. It is especially important to optimize investigation lead-times in view of the constraints of the statute of limitations in disciplinary and judicial matters (see 3.1.), the need to preserve evidence and the truthfulness of witness testimony, and the possible negative repercussions of a disclosure of information;

23 AFA, Guidelines of 12 January 2021, JORF, § 270, p. 34.
24 Labour Code, Article L.2312-8 and Article L.2312-38.

- Guarantee a quality standard for all internal investigations to prevent the risks of case handling inconsistencies from one investigation to the next, by ensuring the traceability of investigations to be able to respond to the audits conducted by the AFA pursuant to Article 17 (III) of the Sapin II Act.

This official procedure should ideally be as comprehensive as possible and could usefully describe:[25]

- The criteria required to trigger an internal investigation and possible exemptions;
- The different steps of the internal investigation procedure;
- The position and role of participants in each step (senior management or its appointed qualified persons, special or *ad hoc* committee, company departments, investigation team, etc.) and the procedures for the disclosure and management of any conflicts of interest;
- The description of the investigation's objectives and scope;
- The format and composition of the investigation team (see 2.2.);
- The investigation methods and resources available (see 2.3.);
- The measures guaranteeing the absence of reprisals, the confidentiality of the identity of the persons involved and of the information gathered as well as the data protection, record keeping and archiving procedures, especially for personal data;
- The criteria that determine action to be taken following the internal investigation.

In the case of a corporate group, a good practice could be to adopt a policy at central level based on guiding principles and stipulating the governance applicable between entities, subsequently adapted in the form of investigation procedures geared to local particularities.

Eventually, a good practice could consist in formalizing an easily accessible "Internal Investigation Charter" for participants detailing the guiding principles for investigators, staff rights in the event of an internal investigation (witnesses, experts and persons implicated) and the conduct expected of them by the employer. It is therefore advisable to ensure the consistency of this charter's provisions with the organisation's internal regulations, its personal data protection policy[26] and the related record of processing activities.[27] This charter could usefully be appended to the internal investigation procedure.

Alternatively, the charter provisions could be included in the internal whistleblowing procedure for companies required to implement such a procedure pursuant to the Sapin II Act.[28]

25 AFA, Guidelines of 12 January 2021, JORF, § 270.
26 Especially regarding the processing of personal data by an internal investigation.
27 In accordance with Article 30 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
28 Sapin II Act, Article 8. I.-B.

2.2. Internal investigation players

Although senior management does not necessarily make the strategic decision to conduct an internal investigation (2.2.1.), several options exist regarding the resources to be marshalled (2.2.2.).

2.2.1. The decision to open an internal investigation

The strategic decision to conduct an internal investigation is the responsibility of the company's senior management or its appointed qualified persons. A special or *ad hoc* committee of these persons can be set up for the most sensitive whistleblower reports to jointly decide on any further action to be taken on an internal whistleblower report and the advisability of opening an investigation to confirm or dismiss the suspicions of corruption.

This special or *ad hoc* committee may, for example, include legal, internal audit, compliance, human resources and financial staff. Checks should be made to ensure, in addition to their expertise, their independence (including any conflicts of interest they may have) in order to guarantee the objectivity of the investigation. Depending on the elements reported, the operational directors or any other qualified persons with appropriate guarantees of independence could sit on or be associated with the committee.

In the event that senior management does not itself make the decision to conduct the internal investigation, it is recommended that it should at least be informed of investigations opened into the most sensitive situations, excepting those in which it is itself implicated.[29] In this case, arrangements could be made for a recusal procedure to refer the case to the supervisory body or one of its specialized committees (audit committee, ethics committee, etc.).

29 AFA, Guidelines of 12 January 2021, JORF, § 274, p. 34.

WHO, IN GROUPS, DECIDES TO OPEN AN INVESTIGATION AND AT WHICH LEVEL OF THE ORGANISATION IS IT CONDUCTED?

Although there are obvious advantages to centralized management of the internal investigation procedure (fuller information for group directors, consistent handling of different investigations, pooling of resources, expertise of central teams who could be assigned to handling such cases, etc.), there can also be drawbacks (limited knowledge of the local legal and cultural environment, risk of legal exposure for the parent company and its management, legal grounds for action, etc.).

The Waserman Act of 21 March 2022[30] authorizes entities with less than 250 employees to pool their whistleblower report reception and handling procedures subject to concordant decision of each entity's relevant management body. Other entities can outsource the whistleblower report reception channel to a third party[31] without affecting the handling of the whistleblower report at their level. The law does not preclude this third-party from being another group company.

The investigation procedure must be managed in a way that remains consistent with the whistleblower reporting system set up when the internal whistleblowing system was deployed.

While management procedures may vary from one group to another in view of the unique nature of each internal investigation, the application of the principle of subsidiarity appears to be a good practice. Consequently, the responsibility for action is incumbent upon the relevant entity closest to the facts to be investigated. This approach is consistent with the fact that any disciplinary sanctions will be imposed by the employer of the implicated employee.

Subject to the independence of its members, a special or *ad hoc* committee of the subsidiary's directors could usefully be set up at local level, which does not prevent specially qualified employees from the parent company's staff (legal, internal audit, etc.) from taking part in the investigation. It could also be a good practice to engage a third party with a command of the local legal environment to conduct the investigation.

Whichever solution is chosen, the group's senior management (or its appointed qualified persons) must be kept informed of the investigation's findings and any further action taken for the most sensitive situations so that it can manage the risk associated with the corruption offences, whose repercussions generally extend beyond a single subsidiary.

2.2.2. Persons conducting the internal investigation

Senior management or the qualified persons it appoints to sit on the special or *ad hoc* committee define, in keeping with the pre-established internal investigation procedure, the composition of the investigation team[32] and the resources to be used. Those must be proportionate to the allegations and their potential repercussions for the business.

Depending on its resources and expertise, the organisation may choose to conduct the internal investigation itself. It may also decide, especially when there is an internal conflict of interest, to appoint a third party or assign a joint team to conduct the investigation. In both of these latter cases, it would be appropriate to appoint a contact person in the company responsible for conducting and overseeing the investigation.

30 Act 2022-401 of 21 March 2022 on improving the protection of whistleblowers, Article 3.
31 Decree 2022-1284 of 3 October 2022, Article 7-I.
32 AFA, Guidelines of 12 January 2021, JORF, § 273, p. 34.

When choosing the members of the investigation team, senior management or its appointed qualified persons should pay close attention to those members' training and expertise, independence of action (in particular the handling of any conflicts of interest they may have, access to useful documents, freedom of choice of people to interview, and freedom in their reporting) and objectivity. When external service providers are engaged, they should ensure that they have the appropriate expertise in internal anti-corruption investigations, labour and criminal law, and compliance with the French procedural guarantees provided for by labour legislation. In the event of engaging a third party, they should pay close attention to preventing any conflicts of interest. If the third party is an attorney, they should ensure that this person is different from the lawyer tasked with defending the company or staff under investigation. In any event, under the current legislation and case-law, regardless of the status of investigation team members, the document drafted following the internal investigation is not protected by any professional secrecy.

Senior management (or the qualified persons it appoints to supervise the investigation) ensures throughout the investigation that all the necessary measures are taken by the investigation team to protect the confidentiality of the investigation and the rights of the staff. It is recommended to give formal expression[33] to these strict confidentiality requirements binding on the people tasked with the investigation,[34] whether they are company staff or third parties (consultants, "forensics" experts, etc.).

If all or part of the internal investigation is outsourced, the services rendered by the selected provider must be monitored regularly for compliance with the contractually defined confidentiality and data protection and storage rules.[35] Lastly, additional guarantees should be provided with respect to staff information. (see 3.2.).

2.3. Conducting the internal investigation

The following developments, both in terms of guiding principles and recommended practices in the light of case law, are aligned with the French legal framework. In this respect, businesses operating internationally are recommended to pay particular attention to the lawfulness, fairness and proportionality of the investigation means used which may, depending on local legislation, be regarded differently by the different jurisdictions.

The internal investigation, which legally stems from the employer's power of direction, allows him to control the performance of the employees' work and to ensure that they are complying with their obligations. Although the internal investigation is not governed by any legal or regulatory provisions, it must be conducted in keeping with certain principles of case law[36] that have emerged from litigation relating to the

33 By means of a reminder to staff of the provisions applicable in the organisation in the internal investigation procedure or the internal investigation charter or a contractual note for third parties.
34 AFA, Guidelines of 12 January 2021, JORF, § 271, p. 34.
35 Ibid., § 272, p. 34.
36 Note, however, that the case-law solutions presented in the cases described in this guide are by definition cases in point and that other interpretations could be made by courts in the future.

exercise of the employer's disciplinary power.[37] Hence, any act of corruption by a member of staff constitutes serious misconduct justifying disciplinary dismissal.[38]

Employers should ensure throughout the investigation compliance with the guiding principles (2.3.1.), especially procedural guarantees (2.3.2.) and the investigation means that may be used (2.3.3.). An internal investigation report detailing the allegations and listing the evidence (appended to the report where appropriate) could usefully be drafted (2.3.4.).

2.3.1. Internal investigation guiding principles

Although the internal anti-corruption investigation may serve as grounds to open a criminal investigation or to inform a criminal investigation already open, the judicial authority alone has the authority to determine the scope of its action and the means to be implemented to establish the existence of an offence and identify the perpetrators.

In the case of facts giving rise to an internal anti-corruption investigation other than the opening of proceedings by a French prosecuting authority, and faced with the revelation of particularly serious acts, businesses may prefer to inform the judicial authority beforehand. This approach, prior to the opening of an internal investigation, is alone capable of preventing any disappearance of evidence and any dissipation of criminal assets that might be seized by a criminal investigation.

The investigation means available to the company, as employer or co-contractor, to gather and preserve the evidence required to ascertain the facts are more limited legally and differ in nature to those available to the prosecution authorities. Given that the principle of freedom of evidence is not absolute in either labour or civil law, the organisation must respect the following guiding principles: not gather evidence by means that are unlawful, unfair or that are disproportionately incompatible with the rights of individuals and individual and collective freedoms.

Non-compliance with these principles can have labour and civil if not criminal repercussions for the company and its management: inadmissibility of the evidence gathered in support of disciplinary action, damages paid to the employee whose rights have been violated, or even a criminal conviction for using unlawful means.

Under French labour law, the business, as the employer, is bound, as are employees, to respect the principle of loyalty resulting from the performance in good faith of the employment contract.[39] As such, employees are bound to cooperate with the investigation conducted by their employer. In return, employers are bound to comply with the procedural guarantees for implicated employees (see 2.3.2.) and to use the investigation means at their disposal proportionate to purpose when investigating staff (see 2.3.3.).

37 French Supreme Court of Appeal Criminal Division, 28 February 2018, Appeal No. 17-81.929.
38 French Supreme Court of Appeal Labour Division, 12 June 1996, Appeal No. 94-44.894.
39 Labour Code, Article L.1222-1.

This principle of proportionality to purpose is stated in Article L.1121-1 of the French Labour Code: "No one may restrict the rights of individuals or individual and collective freedoms unless such restrictions are justified by the nature of the task and proportionate to the aim pursued."

Compliance with this principle is particularly important when it comes to staff's right to privacy. The French Supreme Court of Appeal has consistently held in case law that, "the right to evidence can only justify the production of elements that infringe on privacy if such production is essential to the exercise of this right and the infringement is proportionate to the aim pursued."[40] The Supreme Court of Appeal was followed on this point by the French Supreme Administrative Court, which concluded in a ruling of 2 March 2020 that, "investigations [conducted in the context of an internal investigation] must be justified and proportionate to the allegations behind the investigation and must not excessively infringe on the employee's right to privacy."[41]

It may seem hard to evaluate proportionality to purpose during an internal investigation since the reality of the allegations can only be established after the fact. Nevertheless, the seriousness of a corruption case can authorize the use of considerable investigation means in view of the fact that the European Court of Human Rights recognizes countering corruption as being a matter of public interest[42] and that it has also laid down the principle that the person in charge of the internal investigation must ensure that a balance is struck between the employees' right to respect for their privacy and the proper functioning of the company.[43]

Nevertheless, the internal investigation must be conducted in an impartial manner considering both incriminating and exculpatory evidence.[44] In a recent court ruling, the Paris Court of Appeal ensured that the internal investigation had been conducted in a "meticulous, joint and fair" manner.[45] Especially in the case of an internal anti-corruption investigation, which by definition could give rise to a criminal charge, compliance with the principles of impartiality and fairness must be absolute.

In addition, the principle of discretion, which essentially consists of avoiding needlessly maligning the persons under investigation,[46] derives from both the right to privacy and respect for the presumption of innocence. When the internal investigation ensues from a whistleblower report as provided for by articles 8 and 17 of the Sapin II Act, the confidentiality requirements are much more stringent than merely respecting the abovementioned principle of discretion, in that Article 9 of the Act requires strict confidentiality regarding the identity of the whistleblower, the persons implicated and the information gathered, but also, since the Waserman Act, regarding the identity of third parties mentioned in the whistleblower report.

40 French Supreme Court of Appeal, First Division for Civil Matters, 25 February 2016, Appeal No. 15-12.403.
41 French Supreme Administrative Court, 2 March 2020, Ruling No. 418640.
42 ECHR, 5 May 2020, KÖVESI v. ROMANIA, Application No. 3594/19, § 211.
43 ECHR, 17 October 2019, LOPEZ RIBALDA and others v. Spain, Application Numbers 1874/13, 8567/13.
44 French Supreme Court of Appeal Labour Division, 9 February 2012, Appeal No. 10-26.123.
45 Paris Court of Appeal, 25 January 2018, Appeal No. 15/08177.
46 French Supreme Court of Appeal Labour Division, 9 February 2012, Appeal No. 10-26.123.

Eventually, the retained investigation techniques and especially the use of a certain number of technological means for mass processing of electronically stored information (e-Discovery) involve collecting and processing personal data. They therefore need to comply with the processing rules in force, in particular the General Data Protection Regulation (GDPR)[47] in the European Union and Law No.78-17 of 6 January 1978,[48] known as "*Informatique et Libertés*", in France, based on a few key principles (see box below). If the organisation chooses to outsource these operations requiring the use of technological investigation means, it could usefully refer to the French Data Protection Authority (CNIL) Guide for outsourcing.[49]

DATA COLLECTION AND PERSONAL DATA PROTECTION

Article 5 of the GDPR[50] lays down six key principles relating to the processing of personal data, which all apply to an internal investigation. Fines in the event of non-compliance with these rules can be as high as €20 million or 4% of the business' global turnover (Article 83 GDPR).

1/6 Lawful, fair and transparent data processing

Lawfulness: The company must have an appropriate legal basis for processing personal data. During an internal investigation, processing is based alternatively on the requirement for companies to process whistleblower reports made on the basis of Article 8 or 17 of the Sapin II Act or on its legitimate interest in preventing corruption in the case of an internal investigation that did not result from a whistleblower report.

Transparency: Data subjects must be informed prior to any processing[51] with the exception of two cases:[52] information can be deferred in the event of a risk of destruction or alteration of evidences and it is not required when data need to remain confidential for reasons of professional secrecy.[53]

The right of access to data[54] cannot be exercised when it is liable to violate the rights and freedoms of third parties, such as witnesses interviewed in the context of an internal investigation. To prevent any risk of reprisals, the personal data processing controller can therefore refuse to notify the person under investigation of any information relating to other persons when doing so risks being detrimental to such persons.

47 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.
48 Act 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties.
49 CNIL, Guide for Processors, September 2017.
50 GDPR, Article 5.
51 This information requirement cannot be met by its inclusion in the company's personal data protection policy (circulated to all staff) – the French Data Protection Authority [professional whistleblowing standard – in French only] requires dual information: first, general information when the whistleblowing system is set up and, second, personal notification when a person's data is processed for an internal investigation.
52 These two cases only concern situations where personal data have not been obtained from the data subject (GDPR, Article 14).
53 GDPR, Article 14.
54 These two cases only concern situations where personal data have not been obtained from the data subject (GDPR, Article 14).

2/6 Collection for specified, explicit and legitimate purposes

Data must be collected for the purposes for which their processing is intended and never be further processed in a manner that is incompatible with those purposes. In the case of an internal investigation, data can consequently only be collected in the interest of the investigation and cannot be used for another purpose.

3/6 Collection of adequate and relevant data limited to the procession purpose

The company must comply with a principle of data minimization. As such, it is useful to configure e-Discovery platforms to filter the data that are strictly necessary and objectively useful to the internal investigation.

4/6 Collection of accurate and, if necessary, updated data

The business must comply with a principle of accuracy of collected data. It must take every reasonable step to ensure that data that do not meet this criterion are erased or rectified without delay.

5/6 Data storage limitation

Collected data must be kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed. During an internal anti-corruption investigation conducted further to a whistleblower report, personal data may be kept for the time required for an identified need, such as witness protection or as evidentiary purpose. If the investigation is conducted without a whistleblower report having been made, the data processing controller is responsible for deciding on the data storage periods depending on the purposes of processing. If the data is kept as evidence, the legal period of limitation could, for example, apply.

6/6 Secure data processing[55]

The data collected must be processed in a secure manner, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures[56] based on the principles of integrity and confidentiality.

The risk of destruction of evidence can be associated with the deletion of files and emails or the destruction of paper documents. This risk can be considered as non-existent when two conditions are met: (i) the documents are placed out of the data subject's reach (e.g., in the custody of a trusted third party or in a locked safe); and (ii) the data files are copied in a way that guarantees their inalterability and the copy is saved on a device inaccessible to the implicated persons.

55 See CNIL Guide on Security of Personal Data, factsheets 11, 12 and 17.

56 Examples: user authentication, access authorization management, logging access, encryption and guarantee of the integrity of the data collected, secure archiving, and supervision of data destruction – see CNIL Guide on Security of Personal Data.

2.3.2. Procedural guarantees granted to persons implicated in an internal anti-corruption investigation

→ Informing persons implicated in an investigation

The requirement to inform persons implicated in an internal investigation derives from both the duty of loyalty under French labour law and the obligation of transparency of personal data processing provided for by the GDPR.

Under French labour law, no device can be used to collect personal information on an employee who has not been informed of such beforehand.[57] This loyalty obligation concerns not only the data collection device used, but also its purposes and scope. This information requirement could generate a risk of alteration or destruction of forensic evidence during an internal anti-corruption investigation. Steps should therefore be taken to ensure that the internal investigative work does not contribute to the alteration of this evidence. In practice, the organisation could usefully inform all staff of the possibility of using this type of device, either by informing them individually of the internal investigation procedure and/or the internal investigation charter, or by ensuring their access.

Staff also must be informed of the processing of their personal data in accordance with the principle of transparency.[58] The GDPR requires all persons whose personal data are collected and then processed to be informed of such. Although it is necessary to inform staff, their consent is not required as long as the personal data processing is lawful, such as when it is necessary for the purposes of legitimate interests or for compliance with a legal obligation, as in the case of an internal investigation following a whistleblower report.[59] However, in the case of an investigation conducted following an internal whistleblower report, the report must be sufficiently detailed and precise since the employer must assess its admissibility.[60]

The persons (witnesses, suspected perpetrators and third parties) whose data are collected must be informed as soon as their data are processed, at the latest within one month of obtaining the data,[61] unless there is a risk of loss of validity of evidence, especially if informing the person implicated by the whistleblower report "is likely to seriously impair the achievement of the objectives of that processing."[62] If the investigators consider that there is evidence of such a risk, it is possible to postpone informing the person implicated until the end of the investigation.

In this case, the person must be informed of the processing of their personal data at the end of the investigation. Conversely, if the investigators consider that the risk is moderate, the notification addressed to the person implicated could usefully bear a reminder that the tampering and the destruction of evidence are prosecutable

57 Labour Code, Article L.1222-4.
58 GDPR, Article 5.
59 GDPR, Article 6.
60 Act 2016-1691 of 9 December 2016, Article 8.
61 Or if the personal data are to be used for communication with the data subject or disclosed to another recipient, at the latest when the personal data are first disclosed.
62 GDPR, Articles 14 and 14-5 and CNIL standard of 6 July 2023 on personal data processing for professional whistleblowing systems [in French only].

offences[63] in order to dissuade any attempt to alter evidence or undermine the truthfulness of testimony.[64]

Failure to comply with the duty to inform can have negative consequences. Consequently, the person in charge of the internal investigation must, as far as the requirements of the inquiries permit, give precedence to informing the employee(s) concerned. Indeed, failure to inform employees of the measures taken to collect personal information on them constitutes a breach liable to be sanctioned by the CNIL and may, in certain cases, render the evidence obtained unlawful[65] in the event of its use in a Labour court or civil proceedings. Nevertheless, this recommendation does not necessarily apply in the case of criminal proceedings, especially in the event of internal investigations relating to corruption, since the admissibility of evidence in criminal matters does not depend on information provided in advance to the employee.

Interviews

In accordance with the principle of loyalty in the performance of the employment contract in accordance with Article L.1222-1 of the Labour Code, employees must attend interviews held during their working hours, save legitimate grounds of absence, answer their employer's questions regarding the tasks they have carried out for the business and account for their activities. If an employee fails to attend the interview without legitimate grounds, the employer may draw all consequences from the situation, including disciplinary action.[66] The employee may be sent a summons within a reasonable period of time. Provided that such does not adversely affect the proper conduct of the investigation, the summons could mention the allegations under investigation. It is also possible, subject to the above provision, to give the person heard, prior to the interview, access to the elements of the investigation that directly concern them.

It is preferable for the statement-taking method to be the same for each employee concerned. As such, it is recommended for an interview outline to be prepared in advance, based on the investigation plan, and in keeping with the method provided for by the investigation procedure. This outline could usefully contain the allegations, the key questions to be asked and the list of documents to be submitted to the interviewee during the interview. At the start of the interview, the investigators introduce themselves, state the reason for the interview and could usefully refer the interviewee to the internal investigation charter stipulating the rights and obligations of the investigation participants, in particular guarantees against reprisals and confidentiality guarantees. The presence of at least two investigators at the interview is highly recommended.

63 Article 434-4, 2° of the Criminal Code provides for a three-year prison sentence and a €45,000 fine for "destroying, removing, concealing or altering a public or private document or an item that might assist the detection of a crime or offence, the gathering of proof or the conviction of the guilty parties."

64 Article 434-15 of the Criminal Code provides for a three-year prison sentence and a €45,000 fine for "using promises, offers, gifts, pressure, threats, assault, deceit and trickery during a procedure or pending a court application or defence in order to persuade another person to either make or submit an untruthful statement, declaration or attestation or refrain from making or submitting a statement, declaration or attestation."

65 French Supreme Court of Appeal Labour Division, 10 January 2012, Appeal No. 10-23.482.

66 Pau Court of Appeal, Labour Division, 24 April 2014, Appeal No. 12/01540.

At this stage of the investigation, interviewees do not have the right to be assisted by a staff representative during the interviews. Although the Labour Code provides for employees summoned to a preliminary interview as part of a disciplinary procedure to be assisted by a staff member of their choice,[67] this possibility does not apply to interviews conducted for an internal investigation.[68]

Should the company have decided to have an attorney to conduct the internal investigation, the French National Bar Council (CNB) Guide, based on the Paris Bar Rules of Procedure, stipulates that the lawyer must inform interviewees that they can be assisted or advised by a lawyer if it appears, before or during their interview, that they may be accused of a violation upon completion of the internal investigation.[69] The lawyer tasked with conducting the internal investigation must also state that they are not the attorney of the interviewee and that the elements arising from the interview may be used in disciplinary, civil or even criminal proceedings. These elements could usefully be stated in the summon to the interview.

It is essential to make a distinction between a preliminary interview and an interview conducted as part of an internal investigation. Particular attention should be paid to the reasons for the interview to ensure that it is not seen as a preliminary interview (see 3.1.2.). It has thus been ruled that summoning a member of staff to explain themselves to a panel of investigators appointed by the employer concerning allegations that might give grounds for a disciplinary measure cannot be construed as an interview that is part of a disciplinary procedure and that the employee can consequently not require of an employer to comply with disciplinary procedure rules during an interview conducted as part of an internal investigation.[70]

Particular attention should be paid to the choice of persons to be interviewed. Indeed, although there is no obligation to interview the person under investigation,[71] failure to conduct such an interview could undermine the fair and objective assessment of the situation.[72] The employer must ensure that the sample of persons interviewed during the investigation is sufficient to shed light on the allegations behind the investigation. Nevertheless, the employer is not bound to interview all the staff members who work with an employee under investigation where there is sufficient evidence of wrongdoing.[73] In addition, it could be relevant for the conduct of the internal investigation to interview former staff members or third parties, provided that these persons consent to being interviewed.

Although the employee can refuse to attend the interview and answer the questions and can leave the interview at any time, the employer has the right to take disciplinary action in this event.[74] An employer depriving employee "of their freedom to come and go" "by putting them in an office and telling them to stay there

67 Labour Code, Article L.1332-2.
68 French Supreme Court of Appeal Labour Division, 22 March 2016, Appeal No. 15-10.503.
69 CNB, The French Lawyer and Internal Investigations Guide, 12 June 2020, p. 24.
70 French Supreme Court of Appeal Labour Division, 22 March 2016, Appeal No. 15-10.503.
71 Paris Court of Appeal, 29 August 2018, Appeal No. 16/13810.
72 Rennes Court of Appeal, 25 April 2018, Appeal No. 14/07736.
73 French Supreme Court of Appeal Labour Division, 8 January 2020, Appeal No. 18-20.151.
74 Pau Court of Appeal, Labour Division, 24 April 2014, Appeal No. 12/01540.

until further notice […], placing them at risk of dismissal for misconduct if they attempt to leave" does not constitute the offence of arbitrary detention.[75]

Investigators cannot record the interviews without the consent of the persons concerned[76] when the statements are made in private or confidentially, irrespective of whether the place is private or public.[77] Although it has been ruled that a recording made openly in front of the persons concerned without their objection implies their consent,[78] it is preferable for the employer to obtain written consent from interviewed employees. In the event of non-compliance with these conditions, given that labour court evidence[79] and civil and administrative proceedings evidence must have been obtained fairly, voice recordings made without the employee's knowledge will be dismissed by the relevant courts.[80] However, this consideration does not necessarily apply to criminal proceedings.

It is recommended to respect the principle of discretion applicable to internal investigations[81] when organizing and holding interviews so as to protect the reputation of both implicated employees and the business. A good practice in this respect could be to ensure that interviews are conducted in a neutral place out of sight of company staff. It is also recommended to have interviewed persons sign a document at the beginning of the interview reminding their rights and duties, particularly the personal data rules, stressing out their obligation to respect the confidentiality of the interviews and the investigation.

Any transcript of the interview must be impartial and not constitute "an interpretation by the writer of the discussions that took place."[82] An interview report faithfully reflecting the positions adopted by the interviewee could usefully be drafted following the interview. In certain cases, a record could be drawn up containing all the questions and answers put to and given by the person interviewed. This record could be reviewed and signed by the interviewee for evidentiary reasons,[83] and a mention could be added regarding the interviewee's consent for the document to be produced in court.[84] Regardless of the form of transcript chosen, it is advisable to mention the list of documents provided to the investigators by the employee. Requests for changes expressed by the employee or any details they would like to add following the interview can be included directly into the body of the document or in a reference stating that the employee wished to change or add details to his/her previous statements. In both cases, it is important to ensure the traceability of these changes or additional details. Note, however, that reports and records of interviews are not to be confused with the interviewers' personal notes.

75 French Supreme Court of Appeal Criminal Division, 28 February 2018, Appeal No. 17-81.929.
76 Criminal Code, Article 226-1.
77 French Supreme Court of Appeal Criminal Division, 7 October 1997, Appeal No. 96-81.845.
78 Criminal Code, Article 226-1.
79 French Supreme Court of Appeal Labour Division, 29 January 2008, Appeal No. 06-45.814.
80 French Supreme Court of Appeal, Second Division for Civil Matters, 7 October 2004, Appeal No. 03-12.653 / French Supreme Court of Appeal Labour Division, 29 January 2008, Appeal No. 06-45.814.
81 French Supreme Court of Appeal Labour Division, 9 February 2012, Appeal No. 10-26.123.
82 Paris Court of Appeal, 9 January 2019, Appeal No. 16/15627.
83 CNB, The French Lawyer and Internal Investigations Guide, 12 June 2020, pp. 27 and 29.
84 French Supreme Court of Appeal Labour Division, 4 July 2018, Appeal No. 17-18.241: Judges (industrial tribunal) cannot base their decisions exclusively on anonymous testimony [consent from interviewees to produce the report or record of their interview in court could therefore be required for reasons of evidence].

2.3.3. Investigation means and respect for staff privacy and rights

Under the terms of the general employment relationship between employer and staff in French law, the latter must be informed of the means used to monitor their activities.[85] This information is generally provided when they take up their employment. It may, for example, be specified in their contract or in the internal rules of procedure provided to them. Employees of French businesses covered by an internal investigation must be informed beforehand of all the investigation means used for the internal investigation. No staff activity control technique of which they have not been informed beforehand can be used. In addition to this information requirement, the abovementioned principle (3.1.) of strict proportionality[86] of investigation means used to the aim pursued[87] must lead the person in charge of the investigation to ensure that a balance is constantly struck between the employees' right to respect for their privacy and the proper running of the business.[88] The company should therefore endeavour to minimize the quantity of data collected. One possibility is to proceed with inquiries step by step based first of all on a small number of criteria before possibly extending them. Labour case law has clarified which material elements can be gathered by an internal investigation, in which circumstances and using which means.[89]

Employers therefore have the right to consult documents held by employees in their office, even when they are not present, provided that nothing suggests that they are of a personal nature. Employers can also search an employee's safe reserved exclusively for professional use.[90]

In principle, employers can access all of an employee's professional equipment and its contents. Files stored by employees on their computer hard drives and the content of their work emails are presumed to be professional. Nevertheless, any mention of the word "personal" on these files or in the email subject line overturns this presumption and thereby prohibits the employer from accessing the files.[91, 92] However, the fact of an employee naming the hard drive of their professional computer "personal data" does not make all the data it contains personal.[93]

Lastly, the prohibition on employers accessing employees' personal data may be lifted if the "personal" emails or documents are consulted in the presence of the person concerned or once that person has been duly called.[94]

If the employee's files or emails in their professional email box not identified as personal prove to be private, the employer cannot make use of them to sanction the

85 Labour Code, Article L.1222-4.
86 Paris Court of Appeal, 25 September 2019, Appeal No. 17/13830.
87 French Supreme Court of Appeal, First Division for Civil Matters, 25 February 2016, Appeal No. 15-12.403.
88 ECHR Lopez Ribalda and others v. Spain, 17 October 2019, Application numbers 1874/13, 8567/13.
89 Note, however, that the admissibility of evidence in criminal matters can be more flexible than in civil and labour cases.
90 French Supreme Court of Appeal Labour Division, 21 October 2008, Appeal No. 07-41.513.
91 French Supreme Court of Appeal Labour Division, 16 May 2013, Appeal No. 12-11.866 (Files).
92 French Supreme Court of Appeal Labour Division, 18 October 2011, Appeal No. 10-26.782 / French Supreme Court of Appeal Labour Division, 9 September 2020, Appeal No. 18-20.489 (professional email box).
93 French Supreme Court of Appeal Labour Division, 4 July 2012, Appeal No. 11-12.502 / ECHR Libert v. France – Application Number 588/13.
94 French Supreme Court of Appeal Labour Division, 17 May 2005, Appeal No. 03-40.017.

employee, even if employees have made unauthorized use of the professional equipment assigned to them.[95]

Emails exchanged on a personal email account are personal and private. The employer cannot use them, even if their content concerns company business.[96] The employer can in no event use the content of emails exchanged by an employee on a personal email account to accuse that employee of a breach of his obligation of loyalty.[97]

However, a USB key plugged into a professional computer is presumed to be professional, even if it belongs personally to an employee, when it is connected to an IT tool placed at the employee's disposal by the employer for the performance of their employment contract,[98] even if the employer had prohibited the connection of a personal external device to professional equipment. The employer can therefore access the content of that USB key as part of an internal investigation.

An employee's conversations on an instant messaging service associated with a personal email account are confidential.[99] However, conversations on instant messaging services made available to employees by the business are considered to be professional conversations and their content is therefore not covered by secrecy of correspondence, provided that the content is not private in nature.[100]

Although the use of video surveillance is probably less relevant in the case of an internal anti-corruption investigation, its use is possible in certain circumstances. When a video surveillance system is installed in the workplace, it is imperative that it complies with the rules stipulated by the GDPR[101] regarding personal data processing. Video surveillance is accepted only in certain circumstances. Constant filming of an employee's workstation is disproportionate, aside from particular circumstances that might concern the nature of the assigned tasks,[102] for example in the event of handling items of value or money and in cases of theft already reported. Likewise, video surveillance recordings cannot be used against employees if the device constitutes an invasion of their privacy and is disproportionate to the purpose of ensuring the security of persons and properties.[103]

For example, video surveillance exclusively of the workstations of cashiers in contact with the public for a limited period of ten days does not constitute an invasion of the employees' privacy.[104]

Lastly, regarding human investigation resources, case law has ruled on a number of situations. Thus, the tailing of an employee by a private detective constitutes unlawful evidence, since it is necessarily an invasion of the privacy of the employee in

95 French Supreme Court of Appeal Labour Division, 2 October 2001, Appeal No. 99-42.942 / French Supreme Court of Appeal Labour Division, 5 July 2011, Appeal No. 10-17.284 / French Supreme Court of Appeal Labour Division, 2 October 2011, Appeal No. 99-42.942 / French Supreme Court of Appeal Labour Division, 12 October 2004, Appeal No. 02-40.392.
96 French Supreme Court of Appeal Labour Division, 16 April 2013, Appeal No. 12-15.657.
97 French Supreme Court of Appeal Labour Division, 26 January 2012, Appeal No. 11-10.189.
98 French Supreme Court of Appeal Labour Division, 12 February 2013, Appeal No. 11-28.649.
99 French Supreme Court of Appeal Labour Division, 23 October 2019, Appeal No. 17-28.448.
100 French Supreme Court of Appeal Labour Division, 9 September 2020, Appeal No. 18-20.489.
101 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
102 CNIL Decision of 5 November 2019, MED 2019-025.
103 French Supreme Court of Appeal Labour Division, 23 June 2021, Appeal No. 19-13.856.
104 ECHR Lopez Ribalda and others v. Spain, 17 October 2019, Application numbers 1874/13, 8567/13.

question.[105] Although intrusive means of this nature are to be ruled out, a control of an employee's work in the workplace during working hours by persons from an in-house department in charge of this assignment (e.g. internal audit department) does not constitute unlawful evidence, even if the employee is not informed of such beforehand.[106]

Irrespective of the procedure used, the organisation must ensure that the integrity of the elements gathered is preserved so as not to compromise the effectiveness of any judicial investigation that may be conducted.

2.3.4. The internal investigation report

It is highly recommended to write an internal investigation report. This involves, as stated in the AFA guidelines,[107] stating at least the investigation method used, all the investigative acts, and all of the facts and evidence gathered to substantiate or discredit suspicions. The report also includes a description of the allegations behind the investigation. It includes an appendix with all the evidence gathered.

If the internal investigation is conducted alongside a preliminary inquiry or a judicial inquiry, the report could be made available to the judicial authorities for inclusion in the procedure as a token of the business' willingness to cooperate, opening up the possibility of a judicial public interest agreement (CJIP) for legal entities and of an appropriate judicial measure for individuals. In this regard, the production of an internal investigation report is also an indication of the robustness of the company's anti-corruption compliance program, which the public prosecutor's office will appraise with the assistance of the AFA.

More specifically, if a CJIP is under consideration when an internal investigation is underway, steps need to be taken to ensure that the internal investigation does not interfere with the judicial inquiries in progress during the negotiation period. To this end, the public prosecutor could be informed of the internal investigation measures taken, including all measures taken to access digital documentary information and interviews with witnesses and parties to the alleged misconduct. It is essential for the public prosecutor to be able to determine, when judicial investigations are underway and in the light of the investigation, whether it is necessary to take certain measures in a strictly judicial capacity (such as accessing emails and interviewing suspects and certain witnesses). The attention paid to this recommendation forms a decisive indicator in the assessment of the quality of cooperation provided by the business to help reach a judicial resolution of the case.

Disclosure of the internal investigation report to the implicated employee is not compulsory, including in a disciplinary procedure. Indeed, the principle of the right of due process does not apply at the non-judicial stage of the preliminary interview.[108] Although Article L.1232-3 of the Labour Code requires employers to tell the employee from whom they have need of explanations the grounds for the envisaged sanction

105 French Supreme Court of Appeal, Second Division for Civil Matters, 17 March 2016, Appeal No. 15-11.412.
106 French Supreme Court of Appeal Labour Division, 5 November 2014, Appeal No. 13-18.427.
107 AFA, Guidelines of 12 January 2021, JORF, § 275, p. 34.
108 French Supreme Court of Appeal Labour Division, priority preliminary ruling, 27 February 2013, Appeal No. 12-23.213.

during the preliminary interview, it does not require them to inform the employee of the elements liable to justify the sanction,[109] including the internal investigation report,[110] even if the employee asks to see it.[111]

Nevertheless, the internal investigation report may serve as grounds for a disciplinary sanction even though there is absolutely no obligation to present it to the employees before their preliminary interview.[112] In this regard, it has been ruled that an internal investigation report drawn up without informing or interviewing the incriminated employee does not constitute evidence obtained unfairly. It is lawful evidence,[113] which can be used against the employee. Lastly, the writing of an internal investigation report can, in certain cases, postpone the starting point of the two-month prescriptive period for initiating a disciplinary procedure (see 3.1.2.).

The investigation report must present the facts of the case as precisely as possible.[114] If the business has conducted interviews, the reports or records of those interviews could be provided to the judiciary with all the documents on which they are based.[115] Likewise, it is recommended for the internal investigation report to describe the methodology used to access information – whether direct, digital or documentary – and investigative limitations (e.g. absence of paper or digital archives, legal obstacles, technical problems, etc.). Here again, the presence of this information is a further indication of the reliability and objectivity of the internal investigation report submitted to the judicial authority.

Assuming that the internal investigation finds evidence of what might constitute corruption, it could be useful for the investigation procedure to provide for the report to be submitted solely to authorized persons for them to substantiate the findings before the report is submitted to the relevant company's senior management or the persons it has appointed to decide on any further action to be taken.

109 French Supreme Court of Appeal Labour Division, 18 February 2014, Appeal No. 12-17.557.
110 Paris Court of Appeal, 30 November 2016, Appeal No. 15/01947.
111 French Supreme Court of Appeal Labour Division, 29 June 2022, Appeal No. 20-22.220.
112 Paris Court of Appeal, 29 August 2018, Appeal No. 16/13810.
113 French Supreme Court of Appeal Labour Division, 17 March 2021, Appeal No. 18-25.597.
114 PNF, Guidelines on the implementation of the CJIP, 16 January 2023, p. 9.
115 Ibid., p. 10.

STANDARD FORMAT FOR AN INTERNAL INVESTIGATION REPORT

CONTENTS

INTERNAL INVESTIGATION ENGAGEMENT LETTER

Statement of the precise period, place(s) and person(s)/business unit(s) concerned by the engagement.

ASSIGNMENT ARRANGEMENTS

a) Internal investigation officer – team member(s) conducting the assignment

b) Support: names and tasks of the assistants

c) Practical procedures: travels, interviews conducted, investigation dates, work method and preservation measures put in place

SUMMARY OF THE ASSIGNMENT

DETAILED PRESENTATION OF THE ASSIGNMENT

List of all the actions and operations irrespective of their outcome.

INVESTIGATION FINDINGS

Findings evidenced by the investigation's inquiries.

APPENDICES with detailed contents

The appendices include the documentary evidence and interview reports or records supporting the assignment's findings. A plan of action could also be formalized listing the measures planned to reduce the risk of repeat offences and improve the anti-corruption program.

3. ACTION TO BE TAKEN FOLLOWING THE INTERNAL ANTI-CORRUPTION INVESTIGATION

If the drafted internal investigation report finds evidence of what is liable to constitute a criminal offence or breaches of the anti-corruption code of conduct, it is submitted to senior management, or the relevant body defined in the internal investigation procedure, which is responsible for deciding on any further action to be taken. A legal analysis of the facts ascertained by the report could be conducted by the business' legal adviser to present possible action to be taken further to the investigation. These follow-up actions include immediate decisions with respect to legal and/or disciplinary action (3.1.), updating the company's anti-corruption program if necessary (3.2.) and an appropriate communication strategy based on the findings of the investigation (3.3.).

3.1. Immediate action further to the internal anti-corruption investigation

3.1.1. If the investigation does not confirm the suspicions

When the findings of the internal anti-corruption investigation do not corroborate the suspicions of corruption behind the launch of the investigation, the investigation is closed. The investigation report is archived in a way that guarantees restricted access strictly reserved for authorized persons in compliance with the personal data protection requirements.

If the trigger for the investigation is a whistleblower report made with the whistleblowing system provided for in Article 8 of the Sapin II Act, the whistleblower is informed in writing within three months of the reception of the whistleblower report[116] of the measures planned or taken to assess the accuracy of the allegations and, where appropriate, remedy the situation behind the whistleblower report. The whistleblower must also be informed in writing of the closure of the verification operations when the investigation has not made it possible to corroborate the elements reported, in accordance with the provisions of Article 4, III, 4° of Decree 2022-1284 of 3 October 2022 incorporated in the AFA Guidelines.[117]

When the internal investigation results from the whistleblower report mentioned in the above paragraph, the report and the elements gathered by the investigation can be kept on file. Action taken refers to any decision made to act on the internal whistleblower report. Action is therefore not restricted to disciplinary or legal action and includes, for example, the decision to conduct an internal investigation, the adoption or amendment of internal rules and procedures, and any organizational

116 Or, in the absence of acknowledgement of receipt, within three months of the end of a period of seven working days following the whistleblower report.
117 AFA, Guidelines of 12 January 2021, JORF, § 266, p. 33.

changes made, including those adopted to protect the whistleblower against any potential reprisals.[118]

In this event, the personal data contained in the whistleblower report liable to identify the whistleblower and the persons implicated do not need to be rendered anonymous or destroyed, provided that this retention meets an identified need such as protecting witnesses against reprisals or as evidence.

If the internal investigation is not the result of a whistleblower report as provided for by articles 8 and 17 of the Sapin II Act, the data processing controller could usefully decide on the storage periods for the data gathered by the investigation depending on the processing purposes, for example, by aligning with the period of limitation if the data is kept as evidence.

3.1.2. If the investigation confirms the suspicions

→ Misconduct is attributable to an individual

Evidence provided by the internal investigation of corruption by an individual within the organisation should give rise to the application of disciplinary sanctions provided for in the internal rules of procedure or in any other instrument binding on the employee pursuant to the legislative and regulatory framework, in accordance with the AFA guidelines.[119] Senior management decides on these sanctions.[120] The latter are proportionate to the gravity of the misconduct, as set out in the scale of sanctions stipulated in the disciplinary rules.

In this respect, it should be remembered that the employer has two months from the time it is fully aware of the actual nature and extent of the staff's misconduct[121] to take disciplinary action.[122] Disciplinary action is instigated either by a summons to a preliminary interview,[123] by a precautionary layoff[124] or by the notification of a sanction necessitating no preliminary interview. If the employer decides to take legal action during this two-month period, the statute of limitation is interrupted.[125] The two-month period only starts to run again from the date of the final verdict by the criminal court, if the employer is party to the criminal proceedings, and otherwise from the date on which the employer is informed of the final outcome of the criminal proceedings.

When an internal investigation is necessary to verify the allegations against the employee or the extent of the misconduct: the employer is considered to have knowledge of the wrongdoing at the date of disclosure of the investigation's findings,[126] provided it has opened the investigation within two months of the date on

118 AFA, Guidelines of 12 January 2021, JORF, § 283, p. 35/ CNIL, CNIL standard of 6 July 2023 on personal data processing for professional whistleblowing systems, p. 6, p. 8 [in French only]
119 Ibid., § 159 and § 160, p. 22.
120 Ibid., § 277, p. 34.
121 French Supreme Administrative Court, 20 April 2005, Ruling No. 254909 / French Supreme Court of Appeal Labour Division, 7 November 2006, Appeal No. 04-47.683.
122 Labour Code, Article L.1332-4.
123 French Supreme Court of Appeal Labour Division, 5 February 1997, Appeal No. 94-44.538.
124 French Supreme Court of Appeal Labour Division, 13 January 1993, Appeal No. 90-45.046.
125 Labour Code, Article L.1332-4.
126 French Supreme Court of Appeal Labour Division, 2 June 2017, Appeal No. 15-29.234 / French Supreme Court of Appeal Labour Division, 16 March 2010, Appeal No. 08-44.523.

which the allegations were brought to its attention.[127] Nevertheless, the internal investigation does not always justify postponing the starting date of the period of limitation, especially where there is sufficient evidence of misconduct.[128]

Lastly, opening a preliminary inquiry, which does not initiate public prosecution, does not interrupt the two-month period of limitation for taking disciplinary action.[129]

The criminal statute of limitation is set at six years from the date on which the offence is committed. In the case of covert or hidden criminal offences, the period of limitation only runs from the date on which the offence came to light and is ascertained in circumstances enabling public prosecution, provided that this period does not exceed twelve years from the date of the offence being committed.

→ Legal entities may be held liable in accordance with Article 121-2 of the Criminal Code

The organisation may, at any point in the procedure, including after its conclusion, decide to report the case to the judicial authority, which is not bound by the internal investigation's findings as to the criminal liability of the legal and natural persons implicated.

The business' early reporting in good faith to the judicial authority of offences of which it is aware and disclosure of the internal investigation conducted are likely to constitute elements that will reduce any possible fine under a CJIP.

Nevertheless, any delay in providing the information revealed by the internal investigation and any partial disclosure of the elements gathered by the organisation could be considered as an aggravating circumstance in the calculation of any CJIP fine.

Companies should note that the public prosecutor's office reserves, as at each point in the proceedings, including during negotiations, the right to carry out all necessary actions to investigate and prosecute criminal offences pursuant to the provisions of Article 41 of the Code of Criminal Procedure.

Companies concerned may wish to refer to the PNF Guidelines on the implementation of the CJIP.[130]

127 French Supreme Court of Appeal Labour Division, 25 November 2015, Appeal No. 14-18.661.
128 French Supreme Court of Appeal Labour Division, 17 September 2014, Appeal No. 13-17.382.
129 French Supreme Court of Appeal Labour Division, 13 October 2016, Appeal No. 15-14.006.
130 PNF Guidelines on the implementation of the CJIP, 16 January 2023.

3.1.3. If the investigation findings are inconclusive

Notwithstanding the lack of evidence of corruption, it can sometimes be considered useful to supplement the internal investigation report with an external audit, especially when the suspicion of corruption, despite no hard evidence having been found, cannot be entirely ruled out.

3.2. Updating the anti-corruption program

Aside from the abovementioned possible legal and disciplinary action, the internal investigation may bring to light dysfunctions in the company's anti-corruption program calling for it to be updated to limit the impact and occurrence of such dysfunctions in the future. Subsequent audits and controls should pay particular attention to the areas of vulnerability identified by the internal investigation (3.2.2.) once the corruption detection and prevention measures and procedures have been updated (3.2.1.).

3.2.1. Updating measures and procedures

When the internal investigation results in detecting or corroborating evidence of corruption, the head of the compliance function must assess whether the organisation's anti-corruption program calls for improvement to prevent similar occurrences.[131] It is therefore essential to identify any weaknesses or dysfunctions in the corruption prevention program. Measures planned to prevent repeat offences and improve the program could usefully be formalized in a written action plan.

It would be useful to look into whether similar and hitherto undetected offences may have been committed exploiting the same weaknesses in the prevention and detection program. Any suspicion of such misconduct could, following a preliminary inquiry phase, lead to a supplement to the investigation underway or to the opening of another investigation, if necessary, in view of the new circumstances found.

Depending on the misconduct found, it is recommended to reassess the corruption prevention and detection program's measures and procedures with a view to taking the following actions:

→ Corruption risk mapping

- Assess the need to update corruption risk mapping to:
  - > Include the scenario highlighted by the internal investigation if it is not in the risk assessment;
  - > Change the assessment of gross and net risks if the scenario is already identified, especially the part on existing remediation measures;

131 AFA, Guidelines of 12 January 2021, JORF, § 338, p. 45.

Code of conduct

- Assess the need to update the code of conduct if it does not cover the misconduct revealed by the internal investigation;
- (Re)disseminate the amended version to staff, particularly to those most exposed to risk;
- Send a memorandum from senior management when the updated code of conduct is circulated, stressing the need to scrupulously apply the rules defined in it and to implement the anti-corruption program procedures.

Training

- Assess the need to update training materials to include the scenario brought to light by the internal investigation if it is not on the corruption risk mapping;
- Assess the need to give further training to exposed staff.

Third-party due diligence

- Assess the need to update or improve the third-party due diligence procedure regarding the risk of corruption with a change of method or applicable due diligence measures if the latter failed to identify the third party or parties implicated in the internal investigation as high-risk third parties calling for particular monitoring;
- Assess the need to improve the monitoring procedure for high-risk third parties if the internal investigation reveals that the third party or parties implicated were indeed identified as high-risk third parties, but that a lack of monitoring or dysfunctional monitoring of the third party in the course of the relationship failed to prevent and detect the corruption in question.

Internal whistleblowing system

- Analyse whistleblowing system operations if the case in question shows that the whistleblower report was not able to be submitted through this channel;
- Check the correct implementation of the whistleblowing procedure if it was used in the case in question.

Accounting controls

- Assess the need to update or improve the accounting control procedures in place if they failed to detect the transactions that made it possible to commit the offences ascertained by the internal investigation due to defective design or implementation.

Disciplinary rules

- Where necessary, revise the disciplinary rules if they were unable to impose appropriate sanctions in the case in question.

This assessment of the program following the discovery of corruption should enable a plan of action to be drawn up to sustainably improve program effectiveness and thereby reduce the risk to which the company is exposed.

Should the assessment find human shortcomings in the implementation of policies and procedures, appropriate disciplinary sanctions may be imposed under the terms of the code of conduct appended to the rules of procedure or of any other instrument binding on the employee pursuant to the legislative and regulatory framework.

3.2.2. Subsequent internal controls and audits of the areas of vulnerability identified during the investigation

Particular attention needs to be paid by subsequent internal control campaigns or internal audits to the areas of vulnerability identified during the internal investigation and to monitoring the corrective measures taken for the program to prevent similar occurrences of corruption.

This could include:

- Design and implementation of new controls included in the organisation's internal control system;
- Programming of internal audits to assess the suitability and effectiveness of the anti-corruption program;
- Inclusion in the "regular" internal audit work program of controls designed to prevent the dysfunctions that made it possible to commit the offences ascertained by the internal investigation.

In this case, it is recommended, wherever possible, to avoid restricting the scope of these actions to the activities or subsidiaries within which the offences were committed, but to include activities, processes and geographies that could present a similar risk profile or in which the scenario brought to light by the internal investigation could be reproduced.

Lastly, it could be beneficial to consider scaling up the business' anti-corruption budgetary, human and technical resources following an internal investigation in order to take the abovementioned actions, but also to give consideration to governance of the anti-corruption function and its positioning with respect to senior management. Organisations may refer to the AFA guidelines to put these points into practice.

3.3 Internal communication policy

It is up to the company to inform its staff of the internal investigation, its findings and any further action it intends to take or to keep the internal investigation confidential. However, any absence of sanctions by management following serious misconduct found by the internal investigation could send an implicit message to company staff of its approval of unlawful conduct and could therefore encourage repeat offences.

In addition to imposing sanctions, it is therefore recommended to adopt an internal communication strategy that strikes a balance between the risk of destabilizing teams with respect to the organisation's ethical values and the need to assume ownership as regard to the importance of corruption's prevention and detection.

A detailed communication from senior management could be sent to all or part of the staff reminding them of the company's "zero tolerance" policy of corruption or any breach of the duty of integrity. It should stress the need to scrupulously respect the rules defined in the code of conduct and to implement the anticorruption program procedures. A differentiated communication calling for particular attention on the most sensitive procedures (those whose dysfunctions hindered the prevention of the misconduct found by the internal investigation) could be sent to the managers most exposed to the risk of corruption.

Any communication must be conducted in a way that guarantees the anonymity of the personal data relating to the reported misconduct and any disciplinary sanctions imposed,[132] in keeping with the principles of the presumption of innocence and the right to privacy.

132 AFA, Guidelines of 12 January 2021, JORF, § 345 b, p. 45.

www.agence-francaise-anticorruption.gouv.fr

Development and content
Agence française anticorruption

Design and layout
Desk 53 (www.desk53.com.fr)

March 2023

Contact
Agence française anticorruption
23 avenue d'Italie, 75013 Paris
afa@afa.gouv.fr

For more information
www.agence-francaise-anticorruption.gouv.fr