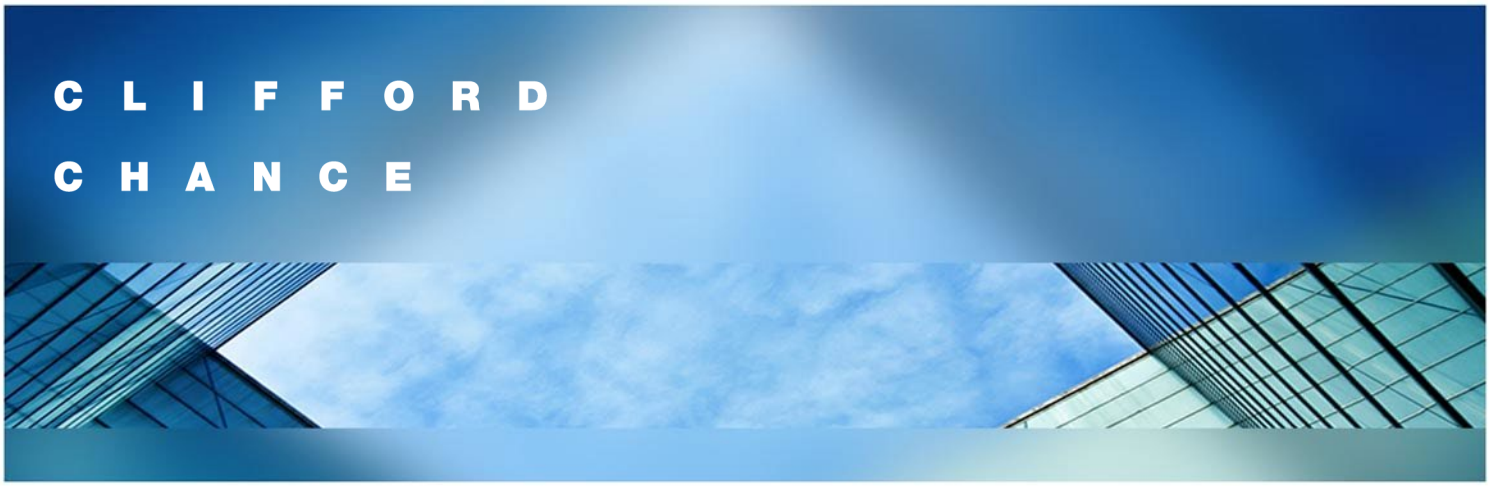

FRENCH AUTHORITIES ISSUE A GUIDE ON INTERNAL INVESTIGATIONS

On 14 March 2023, the French Anti-Corruption Agency (the "**AFA**") and the National Financial Prosecutor's office (*Parquet national financier*, or the "**PNF**") issued a set of guidelines centred on anti-corruption internal investigations (the "**Guide**"). The final Guide comes a year after a draft version was circulated by the AFA and the PNF for public comment and review. Over 350 practitioners supplied critiques as well as suggestions for improvement for consideration by the French authorities.

The final version of the Guide provides guidance to companies on how to conduct internal investigations and recommendations as to best practices. It is important to note that the Guide is dedicated to the conduct of investigations into allegations of anti-corruption as opposed to other alerts that may be raised such as HR or management issues. While the Guide is not binding, given that it is co-signed by both the AFA and the PNF, attention should be paid to its recommendations.

In particular, the Guide lays forth the PNF's expectations of what would be considered a "relevant internal investigation" that would give rise to a potential 20% discount on the additional penalty should the company wish to enter into settlement discussions. The recommendations in the Guide are, therefore, of particular interest to companies that conduct internal investigations with a vision towards a potential settlement agreement and should be read in conjunction with the guidelines published by the PNF on the *convention judiciaire d'intérêt public* (French settlement agreements applicable to certain financial crimes) in January 2023 (for more on CJIPs, see "*CJIP: publication des nouvelle lignes directrices du PNF*" published in the February 2023 edition of

Revue Internationale de la Compliance et de l'Ethique des Affaires).

Key takeaways:

- **Who can most benefit from the Guide**: The Guide is of particular interest to companies who conduct investigations with a view to settle any potential resulting criminal litigation. Though not mandatory as it was under the 2022 draft guide, the Guide emphasizes the benefits that can be reaped from disclosing an investigation report to authorities, including a demonstration of cooperation which will be taken into consideration when determining whether the company can enter into settlement agreement discussions.
- **Key points to bear in mind in the treatment of an alert**:
  - Companies are strongly recommended to develop a detailed internal investigation procedure prior to the launch of any investigation. This will help ensure that alerts are treated in a uniform manner across the company and help protect certain principles in the treatment of the alert (for example, confidentiality and the guarantee that the collection of information will not be done through illicit, disloyal or disproportionate means).
  - The decision to launch an investigation belongs to management or the competent authorities designated by management. The Guide recommends that in the case of a particularly sensitive alert, the decision be made collegially by a committee.
  - The Guide provides a clear answer to the uncertainties created by the whistleblower Directive of 23 October 2019 on the ability for large group of companies to collect and investigate alerts at group level as it clearly states that for bribery-related alerts, it could be more appropriate to handle the investigation at group level and that in any case the group's management must be informed.

BEFORE THE LAUNCH OF AN INVESTIGATION

What information should companies include in an internal investigation policy?

The Guide recommends that companies formalize an internal investigation procedure prior to the launch of any investigative actions. In particular, this policy should include:

- The conditions that need to be satisfied in order to start an internal investigation,
- A description of the steps to be followed during the conduct of an internal investigation,
- The individuals and committees that may play a role in the conduct of internal investigations, along with a description of their roles and responsibilities, and information on how potential conflicts of interest will be declared and mitigated,
- The tools and modes of investigation available to the company,

- The measures companies may deploy to guarantee that the principles of non-retaliation and confidentiality are respected,
- The safeguards the company has in place to ensure the respect of applicable data storage and retention regulations, particularly with respect to personal data, and
- The factors that will be considered when determining the outcome of the investigation, including any potential sanctions that may result.

A formalized internal investigation procedure will allow companies to avoid disparities in the conduct of investigations in different subsidiaries and branches. The Guide also provides that companies can consider implementing a policy applicable at Group level with ancillary policies deployed at local level to account for regional and cultural specificities.

In addition to the applicable procedure, it is recommended that companies adopt a charter that is accessible to all employees that outlines their rights with respect to any potential internal investigation and that reaffirms the principles to be respected in the conduct of an internal investigation.

Through what channels can an alert be raised?

Both practical experience and the Guide demonstrate that alerts can be raised through a variety of channels. These channels can be internal such as through whistleblower hotlines, complaints made directly to managers or the Compliance or Legal Departments, or anomalies identified in internal controls or corporate audits. It is relevant to note that, as is indicated in the Guide, alerts made through the hotline can come from employees, managerial or administrative committees or third parties associated with the company.

Companies may also choose to open an internal investigation upon learning that there is a suspicion of improper behavior from an external source. For example, the company may learn that it is the subject of investigation by French or foreign authorities. The Guide states that companies interested in cooperating with authorities should contact the relevant judicial entity as soon as possible after learning that a judicial inquiry has been opened concerning them to make known their intention to cooperate in order to facilitate the authorities' determination of the benefits or detriments that an internal investigation may cause to the ongoing judicial inquiry.

Who is responsible for determining whether an internal investigation should be launched?

The decision to launch an internal investigation following the receipt of an alert of corruption belongs to management or the competent individuals designated by management. The Guide recommends that for particularly sensitive alerts, the decision of whether or not to conduct an investigation be made collegiately by a committee (either standing or *ad hoc*). The Guide further adds that if the decision to launch an alert is not made by management or its designee, then management should at least be informed of the decision.

CONDUCTING THE INVESTIGATION

A company's obligations with respect to anonymous alerts

The Law No. 2022-401 provides for the treatment of anonymous alerts so long as the misconduct alleged is sufficiently detailed to permit the launch of a review. An anonymous whistleblower whose identity is later revealed benefits from the same protection offered to those who satisfy the criteria of whistleblowers.

Who should conduct the investigation?

Investigations can either be conducted by the competent employees within the company or by an external firm mandated by the company. Regardless of whether internal or external investigators are mandated, corporate management is required to ensure that individuals conducting the investigation are qualified, independent, free from conflicts of interest and have access to the information necessary to complete their mission.

Governing bodies or their designees are responsible for mandating the relevant employees if the investigation is done in-house. Typically, relevant individuals can include members of the Compliance or Legal Department, or of specialized investigation units depending on the size and organization of the company. Alternatively, management may choose to mandate an external law, audit or forensic firm to conduct the investigation.

Limitations imposed on law firms conducting internal investigations

The Guide states that the law firm that conducted the investigation should not be the same as the firm that represents the company in any resulting criminal litigation. This policy was one of the main sources of criticism by practitioners when the 2022 draft guide was circulated for public comment. In particular:

- It is contrary to the right to choose one's legal representation.
- The lawyers that conducted the internal investigation are best placed to provide effective criminal defence given their knowledge of the case as well as of the company's operations more generally.
- This recommendation is inconsistent with what we have witnessed from the PNF thus far as law firms that have assisted with investigations have gone on to represent the company before judicial authorities both in court and in the negotiation of settlement agreements.

It is disappointing that the authorities did not more strongly consider the above critiques when finalizing the Guide.

Treatment of alerts at local level

The Guide provides a clear answer to the uncertainties created by the Whistleblower Directive of 23 October 2019, implemented by the Law of 21 March 2022 (also known as "Waserman Law") and its Regulation (*décret*) of 3 October 2022, on the ability for affiliated entities with more than 250 employees to have their alerts processed at group level.

- The Guide confirms that the collection of alerts can be outsourced to a third party, which can be a group company (for example, the parent company). This is a welcome clarification as the law was not specific on that point.
- With respect to processing, the Guide does not require that the alerts be processed locally but only indicates that this would be good practice. In addition, the Guide indicates that employees of the parent company may participate in the conduct of local investigations.
- In any event, the group's top management must remain informed of the outcome of the investigation and any follow-up given to the most sensitive cases. This clarification is key, although the wording of the draft guide was broader (i.e., the sharing of the outcome was not limited to the most sensitive cases).

What obligations are imposed on the persons conducting the investigation?

The persons conducting the internal investigation are required to adhere to certain principles including:

- Obtaining evidence in good faith through legal means that are proportionate to the alleged misconduct,
- Conducting the investigation with impartiality, and
- Ensuring discretion such as to guarantee the respect of the private lives of the individuals concerned and the presumption of innocence.

What are the constraints on data collection and review?

The collection and treatment of data must respect applicable regulations, including the GDPR. Employees whose data will be collected as part of any review have a right to be informed of the matter beforehand. It is not sufficient for employees to simply receive a general notice informing them of the possibility that their data may be collected and processed. A recommended practice described in the Guide is for companies to issue a general notice on their right to collect data to all employees upon joining the company, and if a situation arises in which review is necessary, to send a second personal notification to concerned employees prior to treatment of their data. The Guide provides for two exceptions to the requirement of personal notice: situations where (1) personal notice will lead to the tampering or even deletion of data or (2) the data is protected by a professional secrecy regime.

How rights must be respected during an interview?

Employees selected for interview should receive formal summons and be provided with sufficient notice before the interview date. Companies may

choose to provide employees with an overview of the scope of the interview and/or with documents that will be raised at interview prior to the meeting.

Under French labour law, employees are obligated to attend interviews if they are summoned by their employers unless they provide a legitimate reason for not doing so. Refusal to attend or to answer questions may result in disciplinary actions against the concerned employee. Unlike with disciplinary interviews, employees do not have the right to the assistance of an employee representative during an internal investigation meeting. However, if the interview is conducted by a law firm and the lawyer considers that there may be findings of wrongdoing with respect to the interviewee, s/he must inform the employee that he s/he has a right to an attorney.

Before turning to substantive questions, interviewers should remind the employee that both the contents of the discussion and the investigation itself are confidential. If the interview is conducted by a law firm, the attorney should reinforce the fact that s/he is the lawyer of the company and not of the employee. It is best practice for interviewees to sign a declaration at the start of the meeting acknowledging they understand their rights and a copy of the meeting minutes at the end confirming that they accurately reflect their statements. Interviews should not be recorded without the consent of the interviewee; if an interviewee does consent, it is advisable to get the confirmation in writing.

What data can companies review within their employees' possession?

Employers have access to the information and data in the possession of their employees. For example, an employer can search the office of an employee even if the latter is not present. In addition, employers can search the equipment made available to the employee by the company, such as professional computers and mobile phones. However, all data contained on a professional device that is labelled as "personal" cannot be reviewed by employers.

In practice, reviewers should be cautious of the handling of personal data. It is good practice to have both tool and human-based safeguards to remove personal data from the review pool. For example, all document to be reviewed should be run through a search tool which can identify and remove documents labelled as "personal." In addition, reviewers should be instructed to immediately remove documents that are of a personal nature if they come across them in the review pool even if not labelled as such.

THE INVESTIGATION REPORT

What information should be included in the report?

The Guide strongly recommends that a formal report be drafted at the close of an investigation. According to the template structure laid out in the Guide, such reports should include the methodology followed during the internal investigation, the concrete investigative steps undertaken, and the elements identified confirming or refuting the alleged misconduct. In addition, we consider it advisable to also record the measures engaged to protect confidentiality and the steps taken to ensure that data privacy regulations were respected to provide a formal trace of the protective measures deployed.

What protection is offered to investigation reports?

The status and protection offered to investigation reports in the 2022 draft guide was a source of debate among practitioners. Some of the revisions in the final Guide respond to the critiques raised but certain elements remain problematic.

***A positive development**:* The 2022 draft guide required companies to handover internal investigation reports to the French authorities, a point which was widely critiqued by practitioners. The final Guide states that companies may provide the report to judicial authorities but are no longer obligated to do so.

This modification goes towards ensuring that companies' defence rights are protected, particularly the right against self-incrimination. In addition, it decreases the risk of a perversion of the internal investigation process in an attempt to avoid findings of wrongdoing that would need to then be disclosed to the authorities.

Nevertheless, the Guide continues to strongly incentivize the voluntary disclosure of investigation reports. In particular, disclosure can be used to demonstrate cooperation with French authorities and will be considered in the company's favour should it seek to enter into a settlement agreement. This is in direct opposition to the practice in the US where "[e]*ligibility for cooperation credit is not predicated upon the waiver of attorney-client privilege or work product protection*" (DOJ Principles of federal prosecution of business organizations, Section 9-28.720). The DOJ guidance on cooperations credit goes on to emphasize that what is key for demonstrating cooperation is the disclosure of relevant facts.

A persisting problem: The Guide considers that investigation reports prepared by external law firms do not benefit from legal privilege. This unfortunate position may weaken the trust between clients and their attorneys, and harm companies' defense strategies. More problematically, this position may have the opposite effect intended by the French authorities in that it may dissuade companies from conducting internal investigations or incentivize a light touch approach to avoid the identification of wrongdoing.

This stance is contrary both to the current French legal regime and that of other jurisdictions. For example:

- The French law governing the protection of defense rights was amended in December 2021 by Law No. 2021-1729. The French Ministry of Justice issued a bulletin (*circulaire*) on 28 February 2022 clarifying certain provisions of the law. The bulletin emphasized that the protection of "**defense litigation privilege**" (*secret de la défense*) is absolute. All documents prepared by an attorney for the defense of her/his client in the context of a criminal case is covered by defense litigation privilege and cannot be seized except in the limited case where the attorney is involved in the wrongdoing. The bulletin also recognized that "**legal advice privilege**" (*secret du conseil*) has been reinforced under the French regime such that it now applies so long as a person has committed or believes s/he has committed an offense even if no criminal proceedings have yet begun.

- The position of UK courts, as exemplified by Serious Fraud Office v Eurasian Natural Resources Corporation Ltd [2017] EWHC 1, is that **litigation privilege** applies to all documents produced during an internal investigation when it is reasonably contemplated that criminal litigation will ensue.

CLOSE OF THE INVESTIGATION

What steps need to be taken if there are *no* findings of wrongdoing?

If there are no findings of wrongdoing, the investigation is formally closed. The investigation report is archived in compliance with the relevant data protection regulations and access to it is strictly limited. The whistleblower is notified of the closure of the matter.

What steps need to be taken if there *are* findings of wrongdoing?

Misconduct by an employee may give rise to disciplinary proceedings, which should be applied in accordance with relevant internal policies and local law. Such proceedings must result in a variety of disciplinary sanctions and potentially criminal sanctions should the underlying facts also result in a criminal case.

Incorporation of lessons learned from internal investigations:

A recommendation that remains consistent in both the draft and final guides is that companies are encouraged to take into account the lessons learned from the investigation in the development of their compliance programs. For example, the Guidelines encourage companies to consider the root causes that led to the wrongdoing and use them to inform revised version of internal policies (such as the Code of Conduct), future versions of the risk map and training programmes.

CLIFFORD CHANCE

CONTACTS

Thomas Baudesson
Partner

T +33 1 4405 5443
E thomas.baudesson @cliffordchance.com

Charles-Henri Boeringer
Partner

T +33 1 4405 2464
E charles-henri.boeringer @cliffordchance.com

Alice Dunoyer de Segonzac
Senior Associate

T +33 0 44 05 5262
E alice.dunoyerdesegonzac @cliffordchance.com

Ann Du
Associate

T +33 0 44 05 5293
E ann.du @cliffordchance.com

Karima Chaïb
Associate

T +33 0 44 05 5219
E karima.chaib @cliffordchance.com

www.cliffordchance.com

Clifford Chance, 1 rue d'Astorg, CS 60058, 75377 Paris Cedex 08, France