the global voice of
the legal profession®

Global Best Practices For Conducting Internal Investigations

Pascale Lagesse
Global Employment Institute
International Bar Association

The International Bar Association (IBA), established in 1947, is the world's leading international organisation of legal practitioners, bar associations and law societies. The IBA influences the development of international law reform and shapes the future of the legal profession throughout the world. It has a membership of more than 80,000 individual lawyers and more than 190 bar associations and law societies spanning more than 160 countries.

The IBA Legal Policy & Research Unit (LPRU) undertakes research and develops initiatives that are relevant to the rule of law, the legal profession and the broader global community. The LPRU engages with IBA members, legal professionals, international organisations, bar associations and governments to ensure innovative, collaborative, informed and effective outcomes. The IBA Legal Practice Division (LPD) is the overarching body responsible for research, dialogue interchange and networking across more than 50 IBA committees and sections concerned with different areas of substantive law.

July 2021

www.ibanet.org/

Contents

Foreword

'*The Rule of Law is the foundation of a civilised society. It establishes a transparent process accessible and equal to all. It ensures adherence to principles that both liberate and protect.*'[1]

The goal of protection and advancement of the rule of law should permeate our lives as legal professionals and inform the way in which we observe and administer domestic and international laws.

Adherence to those aspirations can, however, be difficult when a lawyer must balance priorities, such as when the demands of public policy compete with the need to protect a client's interests, when media calls for the public's 'right to know' conflict with privacy considerations, or when the preservation of client confidentiality under the principles of legal professional privilege is challenged.

These, and other related issues, are addressed in this publication, the stated purpose of which is to provide companies and their legal advisers with practical guidelines for dealing with internal investigations.

As noted in this work (the 'Guidelines'), such an investigation may be instigated for a number of reasons:

- to provide employees with a healthy working environment by identifying and eliminating undesirable work practices, such as bullying and harassment;
- to increase a company's fiscal efficiency by finding and eliminating fraud;
- to ensure regulatory compliance; and
- to respond to whistleblowing.

Investigations under the first three categories are often, but not always, proactive in nature, and may be motivated by a proper desire to improve corporate culture or to address potential weaknesses in internal processes and controls.

A whistleblowing investigation, however, is almost always reactive in nature. A fundamental challenge for a company undertaking an internal whistleblower investigation is to be, and to be seen to be, fair in all aspects of dealing with a whistleblower complaint.

Much has been written about the disgraceful treatment of many corporate whistleblowers over the years. It is well-documented that many have been the subject of personal reprisals and professional vendettas. That sort of treatment should be, and has been, widely condemned. A corporate response that is informed solely by a paradigm of protectiveness should – under contemporary standards of corporate governance, accountability and transparency, give way to an understanding that a commitment by a company to recognise and investigate a whistleblower's genuine complaint appropriately may well be in the company's best interests. It allows early and effective intervention, and the prospect of avoiding or limiting damage to a company's reputation in the marketplace.

Regulators and governments have become increasingly concerned about providing 'whistleblower protection', leading to the increasingly complex domestic and international regulatory environment that is described in some detail later in this report. Experienced commentators have also suggested the implementation of model corporate whistleblower policies that would amount to covenants on the part of companies to recognise and

1 International Bar Association, Rule of Law Resolution, 2005.

respect whistleblowers' rights and protections, including a broad right to disclose information about illegality or misconduct, protection under the law, the right to be treated fairly and the right to be protected from adverse consequences.[2]

Yet, as important as acknowledgement of and protection for a whistleblower is, an internal whistleblower investigation is not all about the whistleblower. It is equally about the company under investigation. That company has rights and protections under the law, and ought to be entitled to expect equality of fairness in the investigation and in the treatment of the outcomes.[3]

This report has been devised to assist practitioners in advising their clients and in acting in the course of such internal investigations, both in domestic and international environments. Important points of principle are addressed, not least of which is the developing area of the ambit of and exceptions to the protection of legal professional privilege.

Importantly, these Guidelines offer practical advice, including handy checklists. Some of these are directed to specific regulatory frameworks such as the European Union's 2016 General Data Protection Regulation, which, among other things, recognises an individual's right to personal data protection; others are of general application. In all instances, the Guidelines are designed to assist lawyers in ensuring that the particular process in which they are engaged is manifestly lawful and patently fair.

I congratulate all members of the Working Group and the individual contributors who have assembled this information in such a user-friendly format. And I respectfully commend these Guidelines as a useful reference tool for lawyers engaged in this important contemporary area of legal practice.

The Honourable Justice Martin Daubney AM
Past Chair, IBA Judges' Forum

2 See, eg, T Devine and T Maassarani, *The Corporate Whistleblower's Survival Guide* (Berrett-Koehler Publishers 2011) 201–203, which proposes a nine-point 'Whistleblower's Bill of Rights and Responsibilities'.

3 Of course, investigations prompted by internal whistleblower complaints are only one source of information that may trigger an internal investigation. Such information may come from a variety of sources, including other employees, compliance officers, auditors, competitors, stakeholders, press reports and other individuals. Inquiries or investigations by regulators also obviously can trigger an internal investigation.

Background, Working Group and Acknowledgements

The IBA Global Employment Institute (GEI) was created in early 2010 as a collaboration between the three Committees of the Human Resources Section of the IBA Legal Practice Division (LPD):

- the Employment and Industrial Relations Law Committee;
- the Diversity and Equality Law Committee; and
- the Immigration and Nationality Law Committee.

Currently chaired by Els de Wind and Gunther Mävers, the GEI's purpose is to develop a global and strategic approach to the main legal issues in the human resources and human capital fields for multinationals and worldwide institutions.

The idea for this project goes back to 2015, when I had the opportunity to serve as the LPD representative to the IBA Public and Professional Interest Division (PPID)/Section of Public and Professional Interest (SPPI) and had the pleasure to work alongside Stephen Denyer, Sarah Hutchinson, Stephen Macliver and many other great people.

Over two years I took part in numerous retreats and business meetings while sitting on the SPPI Council and the Advisory Board. This provided me with a much better understanding of their goals and objectives, but more importantly met some fantastic individuals and made some great friends.

Having enjoyed working with such a fine group of talented people, I began thinking of how we could foster even greater collaboration between the LPD and the PPID/SPPI , and was inspired to develop a joint project that would bring both groups together.

Given the increase in whistleblowing and internal investigations, what better way to do that than to produce together a set of best practices for conducting internal investigations so that in-house lawyers, human resources professionals and companies could have a quick reference tool available to them with the information they need.

I am immensely proud of the incredible collaborative effort between the LPD and PPID Committees on this project. There was so much enthusiasm right from the outset and it was wonderful to see how everyone came together and worked so hard to make this a reality.

This project could not have been possible without the time and effort that everyone put into it. I wish to extend a sincere thank you to all of the members of the Working Group for their wonderful support.

I would also like to express my gratitude to Valentino Armillei, a doctor in law with whom I have worked for the past few years, for his invaluable assistance.

Working group

LPD Committees

- Anti-Corruption Committee: Bruno Cova, Leah Ambler, Francesca Petronio, Leopoldo Pagotto and Jitka Logesova
- Antitrust Committee: Elizabeth Morony and Marc Reysen
- Banking Law Committee: Ewa Butkiewicz, Carlos Melhem, Giuseppe Schiavello, Michael Steen Jensen and Hannes Vallikivi

- Business Crime Committee: Frederick Davis and Kenan Furlong
- Corporate Counsel Forum: Felix Ehrat and Marco Bollini
- Corporate Governance Subcommittee: Damien Zoubek
- Cybercrime Subcommittee: Meg Strickler
- Diversity and Equality Law Committee: Philip Berkowitz and Regina Glaser
- Employment and Industrial Relations Law Committee: Mercedes Balado Bevilacqua, Erika Collins and Peter Talibart
- Intellectual Property and Entertainment Law Committee: Herman Croux and Alexandra Neri
- Litigation Committee: Ira Nishisato, Tom Price and Tim Strong
- Technology Law Committee: Christopher Holder and Martin Schirmbacher

PPID Committees

- Bar Issues Commission: Claudio Visco
- Human Rights Law Committee: Robert Bernstein and Neelim Sultan
- Professional Ethics Committee: Martin Kovnats and Carlos Valls Martinez
- Regulation of Lawyers' Compliance Committee: Iain Miller, Javier Petrantonio and Valentina Zoghbi

Judges' Forum

I would like to extend a very special thank you to the Judges' Forum and in particular its past Chair, the Honourable Justice Martin Daubney, for the interest he showed in this project and for agreeing to write the foreword to these Guidelines, allowing us to take a step back and get a much broader picture of the challenges faced.

Miller & Chevalier

I am tremendously grateful to Homer Moyer and his team at Miller & Chevalier, who agreed to take part in this project and provide the United States perspective. By sharing their experience and expertise in the area of internal investigations, they allowed us to highlight the key differences between the US and different EU jurisdictions and give this guide a truly global dimension. The substantial contribution of unparalleled quality that they provided was invaluable and I cannot thank them enough for their support:

William P Barry
John E Davis
Homer Moyer
Preston L Pugh
Matthew Reinhard
James G Tillen
Andrew T Wise

IBA Global Employment Institute

I would like to express my sincere thanks and appreciation to all of the GEI officers and members who contributed to this project. I would also like to express my gratitude to the current and past Chairs who were involved in this

project since the beginning for all of their support: Graeme Kirk, Anders Etgen Reitz, Dirk Jan Rutgers, Els de Wind and Gunther Mävers.

I would like to express a warm thank you to the following firms and individuals for their help and support:

- Bredin Prat: Valentino Armillei, Karen Clark-Reitenbach and Marguerite Sabatie-Garat
- Debevoise & Plimpton: Andrew Levine and Jane Shvets
- Stetter: Sabine Stetter
- Van Doorne: Jan Leliveld, Vanessa Liem and Els de Wind

I would also like to extend a sincere thank you to the following firms and individuals for their assistance with the Appendix to these Guidelines:

- BonelliErede: Marco Maniscalco, Alessandro Musella and Giovanni Muzina for the Italian input
- Bredin Prat: Marguerite Sabatie-Garat and Valentino Armillei for the French input
- De Brauw: Janneke van der Kroon, Patrick Ploeger and Stefan Sagel for the Dutch input
- Littler Mendelson: Philip Berkowitz for the US input
- Skrine: Selvamalar Alagaratnam and Lee Mei Hooi for the Malaysian input
- Slaughter and May: Ella Williams, Anna Lambourn and Philip Linnard for the United Kingdom input
- Stetter: Sabine Stetter for the German input
- Stikeman Elliott: Patrick L Benaroche for the Canadian input

IBA

Lastly, I am extremely grateful to the IBA for making this project possible.

I wish to extend my heartfelt thanks to Peter Bartlett, who was chairing the Special Projects group at the time and who strongly encouraged the project, as well as Stephen Denyer, Mark Ellis, Jon Grouf and Kieran Pender for their great support.

Pascale Lagesse
IBA Assistant Treasurer
Chair of the Working Group

Executive Summary

Internal investigations. Two words and a new challenge for companies, involving both new responsibilities and flexibility.

Whether they are mandatory or optional, undertaken at a company's initiative or prompted by a public disclosure or action by enforcement authorities, highly regulated or otherwise, carried out by the company or by its lawyers, national or cross-border, in response to a whistleblowing report or not, internal investigations are taking on unprecedented importance.

This shift corresponds to a change in companies' responsibilities as states are overtaken by globalisation. Acts such as corruption, tax fraud or embezzlement are increasingly transnational in scope, so states are relying more on companies to act responsibly and take measures to prevent unlawful behaviour or misconduct. As a result, companies are becoming the main parties in charge of investigating any misconduct related to their business activities. As one compliance officer said: 'Companies are increasingly entrusted with roles which are traditionally carried out by the state.' More generally, there is a worldwide need for transparency.

Companies, especially transnational ones, seem to be able to respond to this greater need for transparency. However, the shift in roles raises questions: how far will countries be prepared to go? More specifically, how much power will countries devolve to companies? Will they tolerate, for instance, companies exercising sovereign rights such as issuing currency? These questions were raised, when Facebook announced it would be launching its own cryptocurrency. Discussions about such powers being exercised both by companies and states may shape one of the most significant challenges of the 21st century, and internal investigations will be one of the key responses to that challenge.

However, in jurisdictions where enforcement authorities already rely heavily on corporate internal investigations, the trend toward empowering companies with state responsibilities does not exist, or is reversed: US courts, for example, have underscored the importance of enforcement authorities conducting their own investigations.

The first and most common reason for conducting an internal investigation remains to investigate suspected, potentially serious, wrongdoing. Accountability for wrongdoing is typically a higher concern than transparency. For example, one of the first questions companies ask when an investigation begins is whether serious wrongdoing that could subject the company to adverse consequences, including criminal liability, may have occurred. If so, an internal investigation is likely.

Whatever the causes and the goals, when internal investigations have a transnational character, they raise similar questions. Managing 'cross-border privilege', making sure the attorney–client relationship is established with each legal entity (potentially) under investigation in each relevant jurisdiction, checking whether it is necessary to hire local attorneys for maximum protection: all these issues are likely to arise more and more frequently.

The internal investigation will have several priorities: identifying the wrongdoing; stopping the wrongdoing (ongoing violations); remediating the wrongdoing; enhancing compliance programmes to prevent recurrences; and considering whether to report the wrongdoing to the relevant authorities. Once a report of miscoduct is received, the company will naturally have to verify the facts disclosed by the internal whistleblower before taking any further actions.

In most cases, this verification will require investigations that, while perfectly acceptable because they are traditionally within the employer's power, will nevertheless have to take into account the constraints affecting the exercise of this power. Indeed, in many jurisdictions, respect for the fundamental rights and freedoms of employees and all third parties involved is essential to make any evidence admissible in court.

Thus, the means of control used by the employer must not restrict the rights and freedoms of employees in ways that are not proportionate to the intended purpose or justified by the nature of the task being performed. The fundamental rights concerned are, in particular, respect for the right to private and family life, freedom of expression and secrecy of private correspondence, among others. These essential limits are not always easy to understand and must lead companies to act with caution and rigour in many jurisdictions. In some countries, such as the US, where the first objective is to complete fact-finding – a prerequisite for addressing improper or unlawful activity by company employees or third parties – the interests of the corporation and its shareholders tend to weigh more heavily than the privacy of employees whose conduct may put the company at risk.

Finally, it seemed appropriate, in view of the diversity of national conceptions of privilege, to carry out a study based on jurisdiction, which has been set out in the Appendix to these Guidelines. However, for ease of reference and for a comparison of the different systems, the choice was made to classify the different responses received by theme.

It is clearly and expressly stated that these Guidelines are not universally applicable to all jurisdictions but that they are primarily and above all to be seen as both a synthesis of the issues raised by internal investigations and as a compendium of suggestions.

Although we believe that the patterns and techniques described here constitute 'best practices', those evaluations are subjective, open to continuing discussion and may need to be adapted in accordance with the applicable local law.

These Guidelines will provide answers to some basic questions, such as:

- When should an internal investigation be conducted?
- Where should an internal investigation be conducted?
- Who should conduct an internal investigation?
- How should an internal investigation be conducted?
- What happens at the end of an internal investigation?

Companies or groups of companies must put reporting procedures in place: while the cost of putting in place a compliance system must be borne by the company, the cost of fraud or misconduct can be immeasurably higher, particularly because of the risks relating to the company's liability.

The simplest way to set up a reporting procedure in a company is to create a single reporting channel wide enough to meet the legal criteria of the various procedures imposed by applicable laws and regulations. Nevertheless, this does not prevent companies from multiplying reporting channels if they so wish or if local regulations impose it. Corporate compliance programmes frequently encourage reports of misconduct through multiple channels, such as through superiors, compliance officers, hotlines and in-house counsel. Although reports are often consolidated in a single office or function, corporations often seek to establish a variety of potential channels to facilitate reporting.

It will be necessary both to encourage people with knowledge of key information to act without fear in the company and to avoid triggering an excessive amount of all types of complaints. It may be appropriate to have a lawyer review the information contained in the documents sent to employees. It is imperative to set out clearly in these documents the exact procedure to follow in order to report facts internally.

There are three main areas where internal investigations can be recommended and are particularly topical at present. These are:

- investigations in cases of moral or sexual harassment, which are very common;
- investigations conducted following corruption or failure to comply with financial, antitrust or banking regulations; and
- investigations following environmental alerts.

It is also clear that the considerations will differ considerably depending on the 'procedural posture' of the investigation (ie, whether it is in response to an irregularity detected by monitoring, a whistleblower complaint or a regulatory request).

In the case of a voluntary investigation, the best approach is to consider some key questions, such as the following, to determine whether to conduct an internal investigation:

- What are the benefits of doing nothing? The company will have to draw up a list of the pros and cons of an investigation, bearing in mind that in some cases a poorly conducted investigation could make the situation worse than if nothing had been done. However, for a US investigation into possible serious wrongdoing, it would be unusual to consider 'doing nothing' because failure to investigate, remediate and disclose would result in penalties if enforcement officials were to learn of the wrongdoing.
- What is the priority (eg, obtaining or securing evidence, or correcting the irregularity)? The focus of the internal investigation will depend on the answer to this question.
- What rules and ethics must the company comply with? Even if the investigation is purely internal and voluntary, certain rules may apply when conducting it (ie, mostly fundamental rights, such as the right to privacy or data protection).
- Internal investigations are an opportunity to rethink the role of legal practitioners. Should counsel only advise the company or should they play a major role in the investigation process by becoming an investigator? The answer will depend on legal privilege, on the area of the investigation and its goals, and on which jurisdiction is competent.

Never assume that privilege will apply; always seek legal advice

In many cases, internal investigations require holding interviews. It should be made clear to the interviewee at the outset that: (1) the interview is not for disciplinary reasons; and (2) if the interviewer is the lawyer of the company, that they represent only the company and not the employee (so called Upjohn warnings in the US). Statements in interviews conducted under French or US jurisdiction are protected by attorney–client privilege, absent waiver by the company through, for example, disclosure of the interview statements. However, neither having been interviewed nor attorney–client privilege forecloses disciplinary action if it is determined that the interviewee was engaged in, or complicit in, wrongdoing.

If the internal investigation is conducted successfully, the final report can become a key piece of evidence before a judge, although an internal investigation's conclusion that allegations have not been proven does not bind the court.

All internal investigations, to be efficient, must meet at each stage of the procedure a general requirement of good faith that implies discretion, impartiality and fair treatment.

With the hope that these Guidelines may be of some use and highlight the main issues arising when it comes to internal investigations, I would like to express my profound gratitude to the Honourable Justice Martin Daubney for recommending and agreeing to write the Foreword to these Guidelines. I also would like to take this opportunity to personally thank all contributors once again.

Pascale Lagesse
Partner, Bredin Prat
IBA Assistant Treasurer
Chair of the Working Group

Introduction: Why Draw Up These Guidelines?

The purpose of these Guidelines is to provide companies with practical advice on internal investigations and help them to adopt the best standards of precaution in order to handle all types of internal investigation efficiently and successfully.

It is clearly stated that these Guidelines are not universally applicable to all jurisdictions but that they are primarily and above all to be seen as both a synthesis of the issues raised by internal investigations and as a compendium of suggestions.

In the context of these Guidelines, 'whistleblowing' refers to internal reporting (ie, a report made within the company).

Except where expressly stated, the Guidelines set out hereafter only deal with internal investigations conducted by companies.

These Guidelines will provide answers to five basic questions:

- Why should an internal investigation be conducted?
- What should companies do to be prepared for an internal investigation?
- What are the mean features of an internal investigation?
- How is an internal investigation carried out?
- What happens at the end of an internal investigation?

The answers to these questions deal with classical aspects of internal investigations and what the company can expect from the internal investigation, but also try to focus on aspects of cross-border internal investigations that are less well-known and can trigger specific problems.

Many general guidelines are relevant as certain issues are common to all investigations, regardless of the field of law:

- evidence collected by an attorney, a private investigator or the company itself;
- whistleblowing;
- interaction with public authorities;
- confidentiality and privilege, especially in the case of cross-border investigations, which are expected to become more frequent in the context of the global economy, for at least two reasons: evidence of an alleged irregularity will very often be found in several countries, and thus public authorities of several countries may react;[4]
- privacy in the workplace;
- employee rights during interviews;
- role of the employee representatives in the investigation; and
- review of documents, among others.

In the respect of this 'multidisciplinary perspective', these Guidelines benefit from the expertise of all the fields

4 See FT Davis, 'How national and local professional rules can mess up an international criminal investigation', *Global Investigations Review*, 17 June 2019.

of law represented by each committee of the IBA.

These Guidelines also have the advantage of being based on extensive feedback from real practitioners from all over the world. The document produced therefore has a fresh and empirical character, which is its main asset and makes it complementary to the studies already published on the subject.[5]

5 See, among several studies, The International Investigations Review (9th ed) The Law Reviews (2019); The Practitioner's Guide to Global Investigations (4th ed) Global Investigations Review (2020); Guide: l'avocat français et les enquêtes internes: CNB/CREA, Assemblée Générale du 12 juin 2020.

Why Conduct Internal Investigations?

Companies are responsible for investigating their own suspected wrongdoing.

This is rather ambiguous because although public authorities demonstrate confidence in companies by entrusting them with the responsibility for investigating any misconduct, they also demonstrate a lack of trust because, in acknowledging there is a need for such investigations, the authorities consider that companies do not have sufficient control over their own activities and actions.

The question of whether to conduct an internal investigation is arising more frequently because of the increase in the number of reasons for conducting internal investigations. Improving the company's efficiency and avoiding liability remains the first and foremost reason. Additional motivations can be to prepare for any investigations by public authorities, and the European and international context of whistleblowing mechanisms.

Increase efficiency and avoid liability for the company

One of the primary reasons that corporate clients elect to conduct an internal investigation is in response to suspected wrongdoing by employees acting on the company's behalf. A threshold step is to evaluate the credibility of a report and the seriousness of the alleged or suspected misconduct to determine whether a formal internal investigation is warranted. Misconduct may be minor or discreet and appropriate for addressing and resolving in a less formal and elaborate manner.

If a report appears credible, and if the alleged wrongdoing could result in harm to the company or criminal liability for the company, an internal investigation is typically a reasonable response. In addition, a report of suspected wrongdoing may also prompt a company to conduct an internal investigation to determine whether there are gaps or failures in its internal controls that allowed wrongdoing to occur (or allowed activities to occur that gave the impression of wrongdoing).

Alleged economic or financial wrongdoings

Companies should not hesitate to implement a compliance system. Even if it is a cost that must be borne by the company, the cost of fraud or any other wrongdoings can be immeasurably higher.

According to a study by the Association of Certified Fraud Examiners (ACFE),[6] an average case of internal fraud costs the company five per cent of its ANNUAL turnover.[7]

Internal fraud consists mainly of: embezzlement; reimbursement of fictitious expenses; unauthorised use of a company car for personal purposes; fictional improvement of sales in order to obtain a bonus; and unjustified sick leave.

For 23.2 per cent of companies, fraud costs more than US$1m. On average, internal fraud is detected only 14 months after the event, particularly because 95 per cent of the perpetrators are 'proactive' and take steps to conceal their actions.[8] Internal investigations are therefore not merely useful but essential.

According to the ACFE study, whistleblowing remains by far the most effective and widespread way of bringing fraud to the knowledge of the employer: 43 per cent of acts of fraud are discovered via a whistleblowing report.[9]

6 Association of Certified Fraud Examiners, 'Report to the Nations', 11th ed (2020). Available at: https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf, accessed 12 April 2021.

7 *Ibid.*

8 *Ibid.*

9 *Ibid.*

At the same time, traditional monitoring and auditing is far less effective than whistleblowing schemes: hierarchical review only detects from 12 per cent of cases of fraud and internal audit detects 15 per cent. As for external auditing, contrary to popular belief, it is even less effective: it detects four per cent of cases of fraud.[10] Another well-known means of becoming aware of alleged wrongdoing is through complaints from customers, service providers or competitors.

However, this does not mean that we must favour whistleblowing to the exclusion of other measures: they are all complementary.[11]

It should be noted that when a reporting hotline is in place in the company, this significantly increases the number of cases reported. According to the ACFE study, companies can be more effective in their fight against fraud both by multiplying the channels for reporting information (eg, hotline, online forms or email) and by training the employees to use these reporting channels.

Alleged 'individual-related' wrongdoings

In addition to suspected wrongdoings related to economic or financial areas, reports of suspected wrongdoings related to individuals (eg, sexual or moral harassment, moral violence, bad management or sexist behaviour) can also lead to internal investigations conducted by companies.

In most cases, internal investigations are useful in identifying and stopping workplace violence (such as moral and sexual harassment or bullying).[12]

Providing a healthy working environment also means preventing bribery, unfair competition and fraud, since employees are more likely to comply with their duty of loyalty when they respect the system of which they are part.

If a whistleblower informs the company of unlawful or inappropriate behaviour, the company must verify the facts and investigate the origin of the reported facts before taking any necessary corrective measures.

In most cases, this verification and research will also require internal investigations.

Preparing for investigations by public authorities

Rise in regulatory authorities with extraterritorial powers

More and more regulations involve internal investigations (anti-corruption or anti-bribery policies) in many jurisdictions. Earlier, it was limited to extraterritorial effects of US regulations, such as the Foreign Corrupt Practices Act of 1977. Yet, step-by-step, all countries have drawn up their own regulations with extraterritorial effects.

France, for example adopted on 27 March 2017 a law that requires all parent companies, French and foreign, to organise a duty of care towards their subsidiaries and ordering companies. As noted by one legal commentator, 'France was tired of seeing its companies prosecuted only by foreign authorities and forced to pay huge fines to foreign treasuries at the expense of the French taxpayer'.[13] This is a view shared by a growing number of other states. Since 2010, French companies have paid more than US$2bn in fines to the US authorities after investigations into violations of the Foreign Corrupt Practices Act.[14] More generally, the size of the fines is

10 *Ibid.*

11 P Lagesse (dir), Le lanceur d'alerte dans tous ses états: *Guide pratique et théorique: Rapp Inst Messine, Nov 2018, 65.* P Lagesse, V Armillei, Le statut du lanceur d'alerte, Etat des lieux et proposition de directive européenne: *Rev Intern de la Complinace et de l'Ethique des Affaires, Apr 2019, étude 64.*

12 See 'Workplace Investigations – Process and enforcement in the age of #MeToo', *Virtual Round Table Series, Employment Working Group* 2019.

13 S L Dreyffus, 'Le Whistleblowing aux Etats-Unis' (January 2018) 1 Cahiers de droit de l'entreprise 43–46.

14 Marie-Stéphanie Servos, 'FCPA : l'ancien cadre d'Alstom partage son expérience' (Option Finance, 20 February 2019), see www.optionfinance.fr/droit-affaires/la-lettre-doption-droit-affaires/la-lettre-du-20-fevrier-2019/fcpa-lancien-cadre-dalstom-partage-son-experience.html accessed 15 March 2021.

increasing exponentially, even in France, as shown by the UBS case in which the Swiss bank was ordered to pay €3.7bn to the tax authorities. This was one of the biggest fines ever imposed by the French courts in a case related to tax evasion.[15] These aspects are a major source of legal harmonisation.

In practice, in the face of legal risk, which is now weighing more heavily on companies because of the authorities' increased regulatory powers in this area, companies will have to consider allocating more funds to compliance, with the challenge for companies being to provide the means to properly handle a whistleblowing case internally. Improving the quality of internal investigations is thus an imperative.

Indeed, companies typically try to conduct their own investigations first, before enforcement authorities initiate a government investigation. Acting first may bring bad news, but it allows companies to get command of the facts, respond and present a more sympathetic picture to enforcement authorities if they become involved.

Training tool for companies

Internal investigations can also serve as an effective training tool for companies so that they can be prepared in case of future investigations carried out by public authorities. In certain fields, the relevant public authorities have extensive powers (eg, competition authorities or financial markets authorities, such as the Securities and Exchange Commission [SEC] in the US or the Autorité des Marchés Financiers [AMF] in France). Powers notably consist of unannounced visits to the company ('dawn raids') and the seizure of documents or emails, among others. Voluntary internal investigations enable companies to respond to this trend.

In some cases, an internal investigation could also help to reduce the penalties imposed on the company by the relevant authority or, in the best case, to avoid liability when cooperation is deemed to be sufficiently efficient. This is why internal investigations are often conducted before or during investigations carried out by authorities.

The administrative authority concerned (such as the SEC, AMF or Competition Authorities) will carry out an inspection of the company, which can be based on documents or be carried out 'on site'.

In general, during dawn raids, the presence of a lawyer specialised in the matter concerned is strongly recommended. Inspectors have a right of access to documents, but sometimes this right has limits, for example, when the documents are privileged (see below) or relate to private life or health data.

It is advisable to be extremely careful because a refusal by the company's manager when access is legally permitted often leads to criminal or administrative sanctions, which can be very significant.

In general, access to documents concerns corporate documents (nominative social declarations, contribution slips, annual regularisation declarations, salary slips, personnel files, employment contracts), accountants (balance sheets, accounting ledgers), tax documents (tax returns, tax notices) and even legal documents (company articles of association, settlement agreements, judgments of employment tribunals).

Public investigators or inspectors can, in most cases, also interview employees of the company.

Government outsourcing a 'public investigation' to the company

In some jurisdictions, such as the US, public authorities may 'outsource' a public investigation to companies. Cooperation provides companies, in particular, an important, often vital, opportunity to reduce the punishment or monetary penalties that may accompany a finding that the company committed a crime or a violation of civil law. Cooperation typically consists of a company's response to requests by authorities for documents and information and regular updates to authorities on the nature and status of the organisation's internal investigation of the alleged violation. Given the priority that US criminal and civil enforcement authorities put

15 Mathieu Delahousse, 'Amende record pour UBS : les leçons d'une affaire hors norme' (L'Obs 20 February 2019), see www.nouvelobs.com/justice/20190220.OBS0567/amende-record-pour-ubs-les-lecons-d-une-affaire-hors-norme.html accessed 15 March 2021.

on the pursuit of culpable individuals, a company's cooperation may pose a risk to individual employees who are investigated for their roles in the violation.

Basic guidelines for companies in the event of an investigation by a public authority

- Do not be hostile to the investigators or interfere as they carry out their tasks: the company is under a legal obligation to cooperate throughout the investigation.
- Do not be too conciliatory. Investigators do not have unlimited powers; they are restricted to the scope of the investigation (time and subject matter) and must comply with the rules regarding professional secrecy.
- Do not hand over documents protected by attorney/client privilege, as this would otherwise result in an unintended waiver of the right to rely on it.
- Do not do anything that could jeopardise the company's position in the event of subsequent proceedings, such as destroying documents or warning other parties.
- Never leave an investigator unaccompanied.
- Always keep a record of what is copied or seized by investigators.
- Draw up a detailed report on the dawn raid afterwards.

Whistleblowing context

Global context

Evidence of a company's alleged wrongdoings might initially come to the attention of the company through a variety of paths, including a whistleblower or compliance hotline call.

Julian Assange, Edward Snowden, Antoine Deltour: everyone recognises at least one of these names. All of them have been described in the press as whistleblowers. Talking about internal investigations necessarily requires talking about whistleblowers as they are one of the main reasons behind the increase in the number of internal investigations being carried out in Europe.[16]

Global regulations on whistleblowing are having a significant impact on companies. There are two contrasting trends in the different jurisdictions:

- In jurisdictions where state regulation is heavy (eg, the EU), countries are increasingly relying on companies to be responsible and take measures to prevent unlawful behaviour or misconduct. Companies are therefore becoming the main parties in charge of investigating any misconduct related to their business activities. As one compliance officer said: 'Companies are increasingly entrusted with roles which are traditionally that of the State'.
- On the other hand, in jurisdictions where state regulation is lighter (eg, the US), the tendency is to increase state intervention. For example, US courts have underscored to enforcement authorities the importance of conducting their own investigations, instead of outsourcing by asking companies to make inquiries or conduct internal investigations on their behalf.

In any case and more generally, there is a worldwide need for transparency that has led to the adoption of various laws and initiatives: the Sarbanes-Oxley Act in 2002 in the US; the 'Sapin 2' Law in 2016 in France to protect whistleblowers; and the Platform to Protect Whistleblowers in Africa.

16 See International Bar Association Legal Policy & Research Unit and Legal Practice Division, 'Whistleblower Protections: a Guide' (April 2018) available at: www.ibanet.org/Document/Default.aspx?DocumentUid=a8bac0a9-ea7e-472d-a48e-ee76cb3cdef8 accessed 12 April 2021..

In addition, on 16 April 2019, the European Parliament adopted the proposal for a European directive discussed since 2016 to impose common minimum standards in all EU countries providing protection against retaliation for whistleblowers reporting breaches.

European context

The European authorities and institutions had been showing increasing interest in whistleblowers. In response to the so-called Trade Secrets Directive (the 'Directive') of 8 June 2016 and further to a request from non-governmental organisations, a proposal for a European directive had been under consideration since 2016 in order to guarantee whistleblower protection in all EU Member States. Unlike many European legislators, whose initial approaches were sector-specific, the objective of the European Commission was to put in place a single EU-wide mechanism. The purpose of a European directive on whistleblower protection is twofold:

- to impose that every EU Member State put in place whistleblower protection; and
- to encourage every EU Member State to harmonise the rules applicable in this area (at least the minimum standards laid down by the directive).

This directive is a first step to harmonisation of whistleblower protection in Europe and therefore of the corresponding internal investigations.

Taking inspiration from the French Sapin 2 Law, the Commission's proposal initially adopted a chronological approach to the whistleblowing procedure (escalation procedure). To qualify for protection, the person reporting a breach must in principle:

- give priority to the internal reporting procedure (step 1);
- then to the administrative or judicial authorities in the event the employer fails to act (step 2); and
- then to public disclosure in the event the authorities fail to act (step 3).

By way of exception, a person may directly make a public disclosure in the event of 'imminent and manifest danger' or in the presence of a 'risk of irreversible damage'.

However, the European Parliament's draft significantly departs from the approach proposed by the European Commission. The European Parliament's draft is based more on Irish and English law, which provide for a more flexible approach: the whistleblower would have the choice of which reporting channel seems most appropriate depending on the seriousness of the breach being reported. Such a system could be a source of considerable legal uncertainty, both for the company and for the whistleblower, especially in Member States where whistleblowing is very rare or where employees' obligations of loyalty to the employer are not very regulated.

In our view, the European Commission's proposal would have been more appropriate as it provides for tiered chronological steps, with exceptions in case of urgency. However, the European Parliament had the final word and the priority given to the internal reporting procedure was absent from the final version adopted on 17 April 2019.

The Directive was adopted on 23 October 2019 and published in the Official Journal of the European Union on 26 November 2019.[17] Member States need to comply with the directive before 17 December 2021. However, for legal entities in the private sector with 50 to 249 workers, the deadline for implementing the obligation to establish internal reporting channels is 17 December 2023.

17 Directive (EU) No 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting on breaches of Union law.

Even in consideration of this directive, which shall no longer impose an internal priority on the alert given by the whistleblower, this does not mean that internal procedures are not compulsory or useful.

As rightly noted, internal whistleblowing procedures protect large corporations: 'If they have these [procedures] in place, the company will usually be the first informed; if they don't have these procedures in place then the authorities are likely to be the first informed.'[18]

Even if European whistleblowers will be able to report the matter directly to the relevant public authorities if they consider it appropriate, the directive still encourages whistleblowers to follow internal reporting channels first where the breach can be effectively addressed within the company.[19] In any case, these whistleblowers will be fully protected.

The enactment of the Directive could pave the way for harmonising standards at an international level. In the future, it could also lead to another directive related to harmonising internal investigations within the European Union. It is indeed almost certain that an increase in the number of cases of whistleblowing will lead to an increase in the number of internal investigations carried out within companies.

As noted in the Preamble to the Directive itself, 'at Union level, reports and public disclosures by whistleblowers are one upstream component of enforcement of Union law and policies: they feed national and Union enforcement systems with information, leading to effective detection, investigation and prosecution of breaches of Union law, thus enhancing transparency and accountability'.[20]

The same trend towards more self-regulation led the European Parliament to adopt a resolution on 10 March 2021 proposing a draft directive to the European Commission on corporate due diligence and corporate accountability.

In particular, Article 4 of this draft directive stipulates that: 'Member States shall lay down rules to ensure that undertakings carry out effective due diligence with respect to potential or actual adverse impacts on human rights, the environment and good governance in their operations and business relationships.'

Moreover, under the directive, Member States have to ensure that a competent authority 'shall have the power to carry out investigations to ensure that undertakings comply with the obligations set out in this Directive, including undertakings which have stated that they have not encountered any potential or actual adverse impact on human rights, the environment or good governance' (Article 13).

This should result in an increase in the number of investigations being conducted by public authorities for companies that have access to the European Union market.

However, the Preamble of the draft directive also states that 'undertakings should first try to address and solve a potential or actual impact on human rights, the environment or good governance in discussion with stakeholders. An undertaking which has leverage to prevent or mitigate the adverse impact should exercise it.'

Thus, at the same time the directive encourages companies to be proactive and take the initiative to conduct their own internal investigation.

18 S Maeder Morvant in 'Whistleblowing: signs of a shifting landscape', *IBA Global Insight* (Feb/Mar 2019) 17–21.

19 See n 17 above, Preamble (47): 'As a principle, therefore, reporting persons should be encouraged to first use the internal channels and report to their employer, if such channels are available to them and can reasonably be expected to work. This is the case, in particular, where the reporting persons believe that the breach can be effectively addressed within the relevant organisation, and that there is no risk of retaliation. This also warrants that legal entities in the private and the public sector establish appropriate internal procedures for receiving and following-up on reports. This encouragement concerns also cases where these channels were established without it being required by Union or national law. This principle should help foster a culture of good communication and corporate social responsibility in organisations, whereby reporting persons are considered as significantly contributing to self-correction and excellence.'

20 *Ibid,* Preamble (2).

What Should Companies Do To Be Prepared For An Internal Investigation?

Reporting channels and how the company is expected to respond

Companies or groups of companies must put report collection procedures in place. The simplest way to set up a procedure for receiving reports in the company is to create a single reception channel wide enough to meet the criteria of the various procedures imposed by applicable laws or regulations. However, it may then be more complicated to sort through the reports. This could encourage companies to keep several separate reporting channels.

In any case, the company must pre-establish a procedure providing for the modalities to gather reports and alerts. It is essential to insist that employees communicate via the 'official' reporting channels (eg, hotline, contact person or dedicated email box) to avoid outside disclosures.

In practice, physical receipt of reports and complaints is a particularly sensitive subject for companies. The process must make it possible to physically receive the information and allow it to be processed, but it must also make it possible for the company to monitor the behaviour of individuals.

Therefore, how the report or complaint is received is an important policy element:

- Do companies need a hotline, a secure server-based mailbox (possible for large companies) or an internal mail service or letterbox (preferred in small and middle-sized companies)?
- Do reports have to be received by one or more persons? This is a very delicate choice for the company. The presence of at least two people who can consult each other seems appropriate, if for no reason other than to exchange and share the burden of such a responsibility. However, if there is an expert or a person with extensive experience in the field of compliance in the company, the opinion may arise of entrusting such person exclusively with the processing of reports and complaints.

The question of calling on the services of external service providers, consulting firms or lawyers deserves serious consideration: is it better to have an internal reporting system within the company or to entrust this to an external service provider? The latter can, for example, be a preferred solution when the company has several sites worldwide. There are considerable advantages to having a service that is accessible 24 hours a day, seven days a week and in the language of the relevant employee of an international group. However, there are disadvantages, especially when the service provider has little knowledge of the company. Poor knowledge of the company, its processes and organisation or the functions of each person, for example, can lead to a superficial investigation report, disconnected from the reality of the facts and, de facto, unusable.

Although some companies prefer to outsource their processes completely, a mixed system has the advantage of balance, especially in large companies. A small, dedicated internal team, with a computer system that is separate from the rest of the company to guarantee independence and confidentiality, could carry out an initial screening of reports and only refer the most sensitive cases to external professionals such as lawyers. This would be a hybrid solution, halfway between internal and external processing of the reports.

Basic guidelines for companies when implementing a reporting channel:

- Do specify what the employees should do if they want to send a report and make this procedure known within the company (ask for precise facts, information or documents in any form, etc).

- Do develop the reflex to forward the report to the relevant person in case of an error (direct or indirect superior, the employer or the reporting procedure 'contact person').
- Do specify how the company should respond to the report.
- Do acknowledge the receipt of the report without delay so that the person reporting the misconduct or breach understands that their complaint is being taken seriously.
- Do inform the author of the report on the reasonable and foreseeable time necessary to examine its admissibility and the manner in which he or she will be informed of any action which may be taken.
- Do not disclose the name of the person issuing the report and of the persons concerned, or the facts on which the report is based, unless this is absolutely necessary for the purposes of checking or processing the report.
- Do destroy or archive the elements of the file likely to allow identification of the person reporting the misconduct or breach and the other persons mentioned in it, within a reasonable time after the closure of all admissibility or verification operations, unless there is a risk of liability.

Information and training tools

Information on the channel for collecting reports and complaints on alleged wrongdoings must be disseminated by any means within the company, in particular by notification, posting or publication, where appropriate on the intranet, in conditions allowing access by staff members, agents and, possibly, by external or occasional workers. This information can also be provided electronically.

The purpose of providing such information is to ensure 'sufficient knowledge' of the systems in use by staff and workers. In principle, there is therefore no question, for the public authorities, of requiring the company train its entire staff in all the technical provisions on reports and complaints. Rather, the objective is to ensure that everyone is aware of the cases in which a report or complaint can be issued, the main features of the procedure to be followed and the related guarantees and sanctions.

The production of 'whistleblower guides', internal to companies and ideally accompanied by practical illustrations, are effective educational tools.

It is therefore essential that all actors are able to react to events that could generate a report or a complaint. Experience shows that the 'best' whistleblower is close to the situation, particularly in terms of 'industrial espionage' because sometimes, only the technician specialised in their subject will be able to recognise a danger or a fault.

However, it is sometimes difficult to interpret the situation:

- Should the company be concerned about having too many complaints or too few?
- Is the absence of complaints a sign of perfect company compliance or does it manifest the fears of potential whistleblowers?

It will be necessary to both: (1) encourage people with knowledge of key information to act without fear in the company; and (2) to avoid triggering an excessive amount of all types of complaints.

In this respect, it may be appropriate to have a lawyer review the information contained in the documents sent to employees. It is imperative to set out clearly in these documents the exact procedure to follow in order to report facts internally.

Similarly, it is essential that the document draw employees' attention to the fact that a report made in 'bad faith' and without following the procedure defined by the company will discredit the person making the complaint.[21] This is an essential element for the proper functioning of reporting systems.

However, even in the case of a disorderly complaint (eg, made orally or made in public) that is made without respecting the channels imposed by any provisions or company rules, such complaint must be processed if the compliance officer considers that the facts are serious enough and could potentially be proven. An internal investigation must be carried out whenever it is in the company's best interest.

Comply with rights to data protection

If the company is subject to the GDPR or other laws modelled on the GDPR

With the European Union General Data Protection Regulation of 27 April 2016 (the GRPR), it can be said, at least within the EU, that a new fundamental right has emerged: the right to personal data protection.

There is a conflict of standards between the absolute need for the company to document the investigation and keep a record of it in order to prove its good conduct on the one hand, and the need to protect personal data on the other.

When processing information in the context of an internal investigation, several measures must be put in place to guarantee this data protection right.

These measures are based on five main principles laid down by the GDPR and set out in Article 5 (1) thereof:

1. companies and public or private entities are bound by an obligation of fairness and transparency in relation to the collection and processing of data;
2. limiting the processing of data to specific and determined purposes;
3. data is limited to that which is necessary to achieve the purposes for which it is being processed;
4. all reasonable measures must be taken to erase or rectify erroneous or incomplete data; and
5. any data that has become without purpose must be deleted when it is no longer necessary for its intended purpose.

Finally, the relevant companies have data security obligations: data processing must be carried out in 'a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.

These key principles are at the heart of the GDPR and are an essential part of all the rules laid down in all European legislation. Compliance with these main key principles is therefore essential to establishing good data processing practice in internal investigations.

Failure to comply with the GDPR, where applicable, may also lead to the application of substantial financial penalties: under Article 83(5)(a), any failure to comply may result in fines of up to €20 million or up to four per cent of the company's or group's annual turnover.

21 In some jurisdictions, such as France, when the appropriate reporting channel has been used, only a report made in total bad faith (ie, with the knowledge that the facts reported are erroneous), may deprive the employee making the report of the protection against dismissal granted to whistleblowers. See, in particular, Cass soc, 8 juill 2020, No 18-13.593.

Basic guidelines for companies subject to the GDPR:

To comply with the various guiding principles defined by the GDPR, the following specific measures can be taken to establish good practices in the processing of personal data:

- Do define and process a limited categories of data: identity, functions and contact details of the issuer of the whistleblowing report; of the persons accused, of the persons involved in the collection or processing of the reports, facts reported, and so on.
- Do not leave the persons involved in the collection or processing of the reports without control: limit their number, train them, establish a reinforced obligation of contractually defined confidentiality, etc.
- Provide all potential users of the reporting system with a clear and complete information on how it works: name of the entity responsible for the system; objectives pursued and areas covered by the potential reports; optional nature of the system and, thus, absence of consequences for employees if the system is not used; any transfers of personal data to another state; existence of a right of access, rectification and opposition for the benefit of persons identified under the system; etc.
- Do state clearly that misuse of the system may expose the whistleblower to disciplinary sanctions as well as legal proceedings, but conversely that the use in good faith of the system, even if the facts subsequently prove to be inaccurate or do not lead to any action, will not expose the whistleblower to any disciplinary sanction.
- After having checked that there is no risk for the company's liability, data relating to a report that does not fall within the scope of the reporting system must be destroyed or archived without delay.
- If disciplinary proceedings or legal proceedings are initiated against the person accused in a report or against the author of a report made in 'bad faith', the data relating to the report shall be kept by the organisation in charge of managing the reports until the end of the procedure.
- Make sure to comply with the GDPR provisions requiring that data transfers from the EU to a legal person established in a non-EU Member State may only take place if the third country in question ensures an adequate level of data protection.[22]
- Try to secure data storage: access to data processing should be by means of an individual identifier and password, regularly renewed, or by any other means of authentication. Each access should be recorded and frequency of access should be monitored.

If the company is not subject to the GDPR or other laws modelled on the GDPR

Outside the GDPR coverage (and the coverage of some other countries' laws modelled on the GDPR), investigating companies face far fewer restrictions on efforts to collect and process information in internal investigations.

Companies in the US, for example, can also generally share such data with third-party service providers, such as outside counsel and auditors, as well as with government regulators and investigatory authorities. Certain laws, such as the US Freedom of Information Act (FOIA), require government authorities to screen certain types of

22 'Sufficient protection' is deemed to exist when the legal entity in which the data recipient works has signed up to the 'Privacy Shield program': 'The EU-US and Swiss-US Privacy Shield Frameworks were designed by the US Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.' (See 'Privacy Shield Overview' www.privacyshield.gov/program-overview accessed 15 March 2021). However, the Court of Justice of the European Union has invalidated the EU-US Privacy Shield, considering that data protection regulations arising from the domestic law of the US on the access and use by US public authorities of data transferred from the European Union are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law (CJEU, 16 July 2020, C-311/18, Schrems, spec s 185).

sensitive data from general public release, but they generally do not inhibit such authorities' use of such data for investigation purposes. Even the most restrictive data privacy law in the US to date does not materially affect a company's ability to collect, process and view information from its employees during an investigation. The relative lack of employee control over employers' use of their personal data under US law is consistent with the general context of 'at-will' employment in the US.

Basic guidelines for companies not subject to the GDPR:

- Do check the applicable local regulations before launching the internal investigation.[23]
- Do not hesitate to engage qualified counsel well versed in the real-world operation of legal regimes.
- If the right to privacy is recognised by international charters or provisions,[24] check if the latter are self-executing in the jurisdictions where the internal investigation takes place.
- Pay attention to the local regulations that could indirectly have an impact on data protection.[25]
- Do make a list of pros and cons concerning the opportunity to voluntarily apply certain obligations of the GDPR to harmonise the rules that will be applicable to the cross-border internal investigation and, thus, to facilitate the exchange of information.

23 Eg, the China Law on Guarding State Secrets and its implementing rules or the Russian Personal Data Law in place since 2015.

24 Eg, Art 12 of the Universal Declaration of Human Rights, Art 17 of the International Covenant on Civil and Political Rights: 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

25 This is often the case of whistleblowing regulations or of some consumer protection regulations.

What Are The Main Features Of An Internal Investigation?

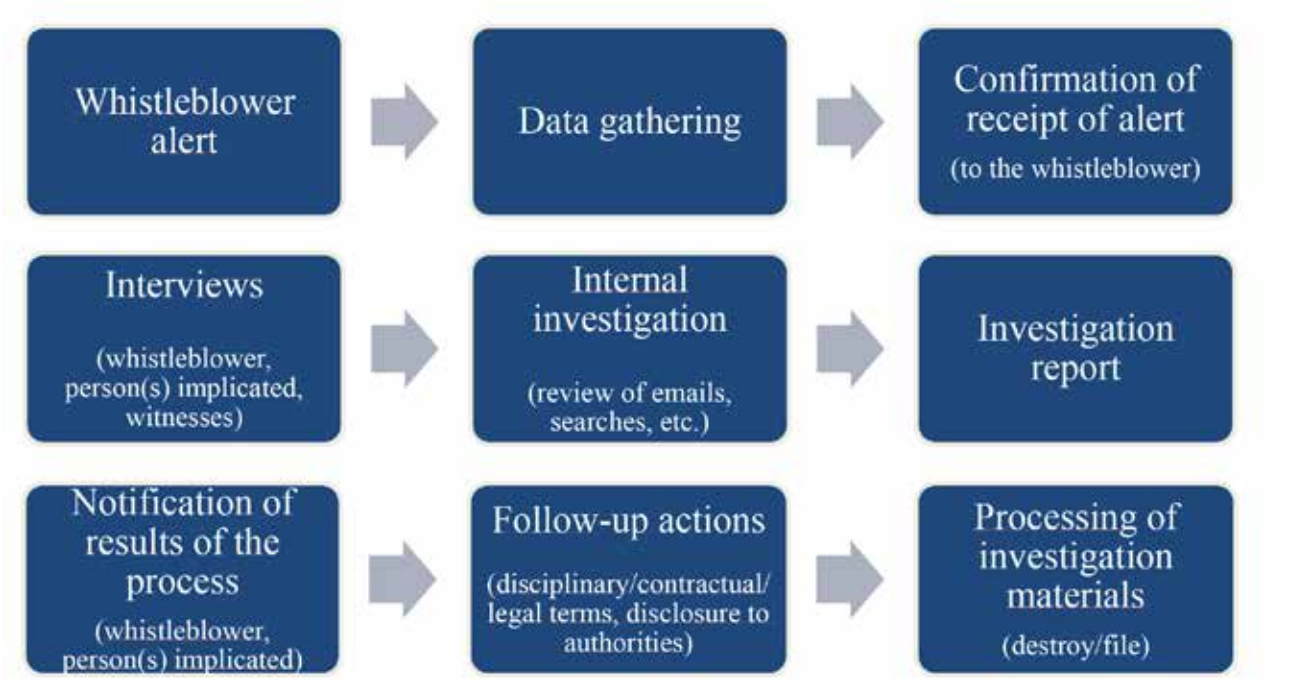
Determine a timeframe

Everybody involved in the internal investigation needs a clear timetable for the internal investigation:

- What is the applicable timeline?
- When is it time-efficient to conduct an internal investigation?

The elaboration of a chronology of facts often proves to be indispensable in certain complex cases that extend over several months or even several years.

Example of timeframe when the internal investigation is triggered by an internal whistleblowing report:



Elaborate the features

Suspected wrongdoings that usually trigger an internal investigation can be divided into three main areas that are particularly topical at present. These are:

- investigations conducted after corruption or poor compliance in financial or banking regulation;
- investigations in cases of moral or sexual harassment, which are very common; and
- investigations after environmental alerts.

The features of the internal investigation will naturally differ according to the area of the alleged wrongdoing.

It is also clear that the features of the internal investigation will differ considerably depending on the 'procedural posture' of the investigation (ie, whether it is in response to a wrongdoing detected by company monitoring, a whistleblower complaint or a regulatory request).

The answers to the following questions should help the company to elaborate the features of the internal investigation and to avoid some of the main pitfalls.

Is the investigation mandatory or optional?

In many jurisdictions, companies must determine whether an internal investigation is mandatory or optional.

The best practice would be to make a list in advance of cases in which an internal investigation would be compulsory, field by field. Compulsory internal investigations are usually linked to anti-corruption, competition or financial regulations.

In some jurisdictions, issues with employee safety can also result in mandatory investigations, particularly when the employee health is at stake (eg, through harassment or violence).[26]

Employee representatives are, in some cases, associated with the procedures.

In the case of an optional investigation, the best practice is to have in mind some key questions to ask when deciding whether or not to conduct the internal investigation:

- What are the benefits of doing nothing? The company will have to draw up a list of the pros and cons of carrying out an investigation, bearing in mind that a poorly conducted investigation can make the situation worse than if nothing had been done.
- What are the priorities (or obtaining or securing evidence, or correcting the irregularity)? Depending on the answer to this question, the focus of the internal investigation will not be the same.
- What rules and ethics does the company have to comply with? Even if the investigation is purely voluntary, certain rules, such as data protection may apply when conducting the investigation, even if it was not compulsory.

Even if the internal investigation is optional (eg, the reported information is anecdotal), it is nevertheless important to plan for the handling of such cases to prevent any potential damage to the company's image. Human resources alerts (personal conflict, complaints about salary or working conditions) often are a grey area between optional and compulsory investigations.

It is important to note that the distinction between 'mandatory or optional' internal investigations is not always relevant. For instance, 'mandatory or optional' internal investigations are not common parlance in the US. Rather, the principal US distinction would be between an internal investigation undertaken at a company's initiative and an investigation prompted by a public disclosure or action by enforcement authorities. These differences may be, in part, semantic, but they may also reflect the fact that investigators may use different tactics in company-instigated investigations than they would when investigating an issue raised in the press or by an enforcement agency.

What about an anonymous whistleblower alert?

In most jurisdictions, there is no obligation to investigate a whistleblower alert submitted anonymously. The whistleblower must identify themselves and the company should not encourage people with a need to use the reporting channel to do so anonymously. In practice, investigating anonymous alerts is not prohibited: it is wise to examine these anonymous whistleblower alerts to verify their truthfulness and to deal with any potential liability issues for the company, as in the case of all voluntary internal investigations.

26 See in France, Cass soc, 27 nov 2019, No 18-10.551: *JCP S 2020, 1011, note V Armillei*, concerning the obligation to conduct an internal investigation in case of suspicion of moral harassment.

It is essential for the company to identify, before any decision is taken, where the complaint comes from without illegally trying to identify the whistleblower behind an anonymous alert.

The complaint can come from outside the company (eg, the media, subcontractor's accountants or clients) or from within the company (legal, compliance or ethics department, corporate security, IT, employee representatives or employees).

In principle, an investigation conducted after an internal complaint can be more flexible.

What about preventive internal investigations?

Even if no tangible element seems to generate a need to investigate internally, regular investigations can be launched, in particular to prevent the risks and assess of potential liability exposure.

In such situations, the internal investigation approaches or, depending on the applicable jurisdictions, mostly identifies itself as audits.

Define the scope

Any complaint received by the company outside the official reporting channels it has set up must be immediately forwarded to the relevant authority within the company. Ideally, this kind of situation should not happen often: by informing and training employees about the reporting systems at their disposal (eg, hotline or dedicated email), it is possible to considerably reduce reports outside the channels put in place by the company.

Once the right person has the information, the next step is to define the scope in the internal investigation. Even though it is always difficult to predetermine what should or should not be investigated, an initial scope must be identified.

The question of a broader scope will be raised naturally if the first was too narrow.

It could be:

- a mere branch;
- a business unit;
- a particular location;
- the whole company;
- one or several subsidiaries;
- the whole group; or
- national or cross-border.

With regard to the last point, several elements can trigger a cross-border investigation:

- Did the facts to be investigated take place in a foreign state?
- Are any or all of the persons concerned abroad?
- Is all or part of the information to be retrieved located abroad?
- Can the facts, even if they took place locally, justify the interference of a foreign authority?

Sometimes, when the internal investigation is compulsory, the perimeter is defined by the legal or regulatory provisions. However, the company will usually have to take the lead on that question and determine itself the appropriate perimeter.

The relevant period to be investigated also needs to be determined. Two situations could be contemplated:

- when the investigation concerns individuals, a narrow scope should be preferred at the very beginning, in particular to try to protect confidentiality; and
- when the investigation concerns material or financial exposure, a broader perimeter can be adopted, and then reduced if needed.

Choosing the right scope of the investigation shows a certain degree of good faith on the part of the company. A perimeter error is not always fatal if it is corrected during the investigation.

Choose the team

General considerations

Having defined the perimeter, selecting the right team is crucial to the investigation. Practice has shown that every case is unique and has its own specific circumstances. There is no 'one size fits all' approach.

The composition of the team will depend on the purpose of the investigation, whether to uncover harassment, discrimination, violence, threats, safety, regulatory, financial, theft, criminal activity or fraud. It will also depend on the objectives of the investigation.

The only crucial rule is to try, to the extent possible, not to have people potentially targeted by the complaint or the investigation involved in the investigation progress.

Regardless of the type of investigator selected, it is essential that they demonstrate certain qualities, such as the ability to interview, analyse, organise, write and practise active listening. The investigator must be a good communicator and must be able to manage difficult people or situations. They must be an example in terms of credibility and impartiality. The success of the internal investigation depends on it.

The investigator must never suggest that the internal investigation is useless, minimise the facts reported, commit to a closing date for the investigation, promise that there will be no sanctions, give a personal opinions or draw conclusions before all the facts have been verified.

The main objective remains to ensure the independence of the team or at least to create a high perception of independency.

The key people in the investigation team can be defined in a pre-established procedure. It is good practice to give decision-makers the possibility to set up, on a case-by-case basis, the team most appropriate to the situation.

In most jurisdictions, companies have the option to outsource the collection of complaints or reports and the investigations by appointing a contact from outside the company. The elements to be taken into consideration when appointing the contact, whether internal or external, are that they have, by virtue of their position, the competence, authority and sufficient resources to carry out the required tasks. It may be a natural person or an entity, with or without legal personality.

Flexibility is welcome in view of the diversity of practices across companies of different sizes and sectors. Thus, the possibility that an unincorporated entity may be designated as a contact allows, in our view, for the company to designate a 'department'. Such a choice makes it possible to dilute individual responsibility, which is likely to lead to a more serene management of the upcoming investigation.

On the other hand, the appointment of a natural person who meets the conditions of competence, authority and resources may, in certain cases, help to exempt the company more easily from possible liability.

In some sectors where it is difficult to find individuals with no conflicting interests, one solution could be to constitute a team using the company's retirees, as their experience is likely to be recognised by the teams, or managers at the end of their careers, who are potentially less sensitive to 'returning the favour'.

In short, there are two types of actors: those who can potentially join the team of investigators and those whose participation is best limited to ad hoc support according to their specific skills.

Who should be in the investigation team?

Members of management?

Before laws were adopted to regulate the investigation process, reports naturally reached the company despite the lack of guidance and formalised procedures. The treatment carried out was then largely empirical. Two essential modes of reporting coexisted before the generalisation of whistleblowing or reporting channels' procedures:

- the anonymous (or not) letter; or
- the unexpected discovery of suspicious facts following audit, accounting or managerial review missions.

In the absence of any formalised procedure, it was often the responsibility of a manager or the chief executive to work on reporting and investigate more informally.

Nevertheless, the presence of a company representative or corporate officers on the investigation team raises the question of impartiality. It is therefore recommended that the investigation team should not include members of the board or managers of the company so that the investigation can be carried out with a certain extent of impartiality.

That consideration is even greater when there is a risk that directors, officers, or senior management were involved in misconduct or failed to identify, deter and remediate misconduct.

Auditors or accountants?

Large-scale investigations conducted without coordination are not particularly effective. Investigations are sometimes conducted without communicating to the investigators what they are supposed to be looking for, which obviously does not achieve the desired results. Targeted use of investigations carried out by auditors is better.

In the case of complex financial frauds, the involvement of the company's accounting departments is essential. However, it is not necessarily mandatory to include them in the investigation team. In the same vein, the company may consider hiring forensic accountants or other third-party experts.

Corporate security personnel?

Corporate security services may be added to the investigation team, particularly when it is suspected that a competitor or a foreign power has attacked the company (eg, poaching customers, fictitious complaints or fake news, unfair competition or data theft).

Human resources?

The human resources department will in many cases want to be systematically involved in the investigation procedure. They generally consider this to be part of their 'domain'. However, this should not be assumed and any preconceived ideas should be avoided.

The relevance of the investigation team members should not be sacrificed because of certain established practices or the influence of certain departments. The effectiveness of the investigation significantly depends on it.

Also, members of the human resources department can be integrated into the team, on a case-by-case basis, when issues directly related to personnel management (eg, harassment or wellbeing at work) are involved.

Whoever is chosen to be in the investigation team, the key question is: do they have enough resources and time to conduct an internal investigation?

External/in-house counsel?

Internal investigations are an opportunity to rethink the role of legal practitioners.

Should counsel only advise the company or should they play a major role in the investigation process by becoming an investigator? The answer will depend on legal privilege and on which jurisdiction is competent. (See below, 'What about legal privilege during an internal investigation?')

To secure counsel's role and the integrity of the investigation report, the counsel's letter of engagement could provide that the lawyer's appointment cannot be revoked while the investigation process is in progress, so that they cannot be removed from the investigation team if the investigators suspect people who were involved in appointing the lawyer and who could dismiss them. Such a recommendation is not relevant in all jurisdictions, for example, the US, and merits consideration on a case-by-case basis.

In the US, the prospect of the disclosure of the internal investigation's findings to public authorities underlines the importance of ensuring that internal investigations are independent and insulated from possible influence by company management. This concern greatly increases the use of outside counsel to conduct investigations.

Even outside the US, companies are increasingly inclined to retain outside counsel to conduct internal investigations on their behalf. They may do so because they wish to strengthen their claim that the internal investigation is protected by attorney–client privilege or because they believe the investigation will be more independent, and it will be perceived as being independent if conducted by an investigator who is not a company employee. That an internal investigation is credible and objective to the outside world can be important because internal corporate investigations do not always remain internal. Particularly in the US, a thorough independent investigation performed by outside counsel can sometimes mean the difference between an indictment or penalties and a favourable resolution for a company facing a government inquiry.

Moreover, in all jurisdictions, experienced, qualified outside counsel may be helpful in identifying issues, evaluating the conduct of personnel and restoring trust with regulators, external auditors and investors. Although not every investigation requires the involvement of independent counsel, failure to take steps to ensure the independence of an important investigation can ultimately waste time and resources and diminish credibility. The concern that drives the need for independent investigations is that undue pressure might otherwise be brought to bear on the investigator by the company.

Basic guidelines for companies when assessing the need for consulting independent outside counsel:

- Do consider hiring an outside counsel when the nature of the allegation(s) at issue is legally consequential, financially consequential or implicates senior management.
- Do take into account the potential reputational impact of the issues under investigation.
- Do consider hiring an outside counsel when cooperation with or disclosure to public authorities is or will be expected.

- Do not necessarily exclude hiring the company's usual outside counsel: outside counsel who have previously done work for the company have acquired an understanding of company operations and processes or can be trusted based on their prior work or dealings with regulators.[27]

Legal privilege during an internal investigation

This topic should be taken into consideration at the earliest opportunity when deciding how to investigate, who to involve and how to structure the investigation.

Indeed, professional and legal privilege rules do not ignore borders: 'Lawyers often bring with them the professional rules of their home jurisdiction and then confront the rules applicable to the places where the investigation is taking place. The differences among these rules – and more importantly, among practices in each country – can create subtle but important problems.'[28]

It is imperative to distinguish here between the two approaches: that allowing lawyers to be both counsel and investigators of the company, and that requiring lawyers to choose between the two roles.

In term of ethics, a recurrent question that arises is whether a lawyer can still advise the company when they are investigating it. Very different answers have been adopted depending on the jurisdiction.

In the English-speaking world, the advisory services provided by lawyers have traditionally included participating in internal investigations for their clients. The choice to entrust the investigation to a lawyer can allow the company to keep better control over the procedure despite such outsourcing, thanks to legal privilege.

However, even in the jurisdictions where investigating a company was not considered as falling within the traditional field of the lawyer's practice, a change in mentality has eventually taken place, leading to a recent modification of the rules, such as in France.

In 2016, for the first time, the Paris Bar Association agreed to allow Parisian lawyers to be investigators under strict conditions.[29] In principle, if a lawyer investigates a company, they can act as lead counsel for that company, as long as they act exclusively in the capacity as counsel and not as 'a third-party expert'.

To be covered by professional secrecy, the internal investigation must fall within the scope of the lawyer's assistance and advice mission.[30]

After some debates, the Paris Bar Association confirmed in 2019 that lawyers may conduct internal investigations for a company that is their client and that the internal investigation would, in principle, be covered by legal privilege.[31]

To conclude, even if the general trend is towards the admission of internal investigations conducted by lawyers, care must always be taken to ensure that this is the case under local jurisdiction and, above all, that the investigation is in principle covered by privilege.

27 The experience of having previously worked for the company or its board can produce efficiencies and savings in time and resources. However, companies tend to balance these potential benefits against whether regulators, external auditors and shareholders will view the investigation itself as independent and credible.

28 F T Davis, 'How national and local professional rules can mess up an international criminal investigation' (Global Investigations Review 17 June 2019) see https://globalinvestigationsreview.com/how-national-and-local-professional-rules-can-mess-international-criminal-investigation accessed 12 April 2021.

29 Conseil de l'Ordre, Vademecum de l'avocat chargé d'une enquête interne, adopted 13 September 2016, Annexe XXIV of RIN.

30 *Ibid.*

31 Conseil de l'Ordre, Vademecum de l'avocat chargé d'une enquête interne, adopted 10 December 2019 and published 20 May 2020, Annexe XXIV of RIN.

Basic guidelines for companies when dealing with legal privilege in the context of an internal investigation:

In light of the differing scope of legal privilege across jurisdictions,[32] some global guidelines are:

- Do not assume that privilege will apply; always seek legal advice.
- Engage lawyers, whether in-house or external, to carry out the investigation to maximise the likelihood that privilege will apply.
- Check carefully when the internal investigation should begin and whether any protection of its results should be provided for at that stage.
- At the outset of the matter, think about who the 'client' is for the purposes of giving instructions to lawyers; revisit this assessment as the matter develops or when the internal team changes.
- Avoid creating unnecessary documents. Consider whether information can be shared orally instead; mark any documents that are privileged as 'privileged and confidential'.
- Key to maintaining privilege is maintaining confidentiality. If information is no longer confidential, it is also automatically no longer privileged. Only share privileged information on a need-to-know basis and only on confidential terms – for example, do not put people on copy of emails containing privileged information when it is not absolutely necessary, or ask the lawyer to be the intermediary to share the information.
- If litigation is reasonably in prospect, document that fact because it may help to evidence that litigation privilege applies; revisit this question as the investigation progresses.
- Carry out a thorough review of contemporaneous documents before speaking to witnesses. This increases the chance that litigation privilege will apply by the time questions are put to witnesses.
- Make sure that the lawyer (external or in-house) is not being asked to investigate their own work.
- Pay particular attention if impartiality is required with regard to the company's managers.
- If the legal provisions of a jurisdiction are unclear about whether attorney–client privilege applies to in-house counsel, consider using external counsel in addition.
- In case of cross-border internal investigation, make sure the attorney–client relationship is established with each legal entity (potentially) under investigation in each relevant jurisdiction and check whether it is necessary to hire local attorneys for maximum protection.
- In the case of a cross-border internal investigation, when a lawyer is registered with several Bars, both local and foreign, professional secrecies are cumulative and therefore lead the lawyer concerned to submit to or take advantage of a cumulative or alternative application, locally or abroad, depending on the circumstances.
- In the case of a cross-border internal investigation, consult the possible conflict of rules of the different jurisdictions in which the lawyer is registered and bear in mind that a local public authority may not recognise the regime applicable to a foreign professional secrecy or conversely with local professional secrecy vis-à-vis a foreign authority.
- In any case, in a cross-border context, discuss with your client at the beginning of the investigation the rules applicable to professional secrecy to maximise the protections that these rules can provide.

32 See the Appendix below.

How is an internal investigation carried out?

Organising the tasks

It is important to prepare the internal investigation to avoid errors, particularly with regard to the communication or the safeguarding of evidence, that could compromise the investigation. It is therefore crucial to define the main features of the future internal investigation.

In particular, the order of the tasks to be carried out should be determined. Is it necessary to start with the hearings or the review of documents?

The answer may depend on the subject matter of the investigation. In principle, it is advisable to first review the documentation before organising interviews, particularly to avoid the destruction of certain documents by ill-intentioned employees or by those wishing to erase the traces of an alleged wrongdoing on their part.

Sometimes, however, it is possible to start with the interviews, especially in the case of harassment, as in this case there may be no documents to review.

If the decision is taken to conduct the documentation review after the interviews, it could be useful to ask the employees involved to sign a document stating that they have a duty to preserve and retain documents, meaning that if they deleted or destroyed any type of documents they would be acting against the company and in breach of the law. Discuss pros and cons of such action as it may further jeopardise confidentiality.

Basic guidelines for companies when collecting information and assessing sources and priorities:

- Contact the person who reported the facts to obtain a more detailed explanation.
- Determine how the person who reported the facts became aware of this information, the persons potentially involved, the starting date of the facts, whether the facts are ongoing and other persons who are aware of the facts.
- Do take the time to assess the reliability of the report.
- Determine the presence of possible victims and the actions to be taken to protect them.
- Determine the involvement of the direct or indirect supervisors of the employee suspected of having committed the alleged wrongdoing.
- Remember to check whether the reported facts or other similar facts have already been dealt with by the compliance department.
- Plan a provisional timetable for the internal investigation and determine, step-by-step, the actions to be carried out.
- Ensure that the team has the necessary resources and expertise.

Reviewing documents

There are two opposing models for document review.

In the US model (and other jurisdictions that have similar rules), courts recognise the right of private employers to require employees to cooperate and participate in good faith in any lawful employer-led internal investigation

about on-the-job conduct.[33] In the US, an employee's duty to cooperate is often referenced in an employer's handbook, investigations protocol or other employment policy, making it clear that the employee is required to fully cooperate in any matter in which they are directly or indirectly involved. With the exception of the relatively few employees who are unionised, courts have consistently held that private at-will employees may be disciplined or terminated for failure to cooperate with an employer's investigation.

As courts have noted: 'There would be a complete breakdown in the regulation of many areas of business if employers did not carry most of the load of keeping their employees in line and have the sanction of discharge for refusal to answer what is essential to that end.'[34] In this system, the employee can almost never object to the review of documents even though some may contain elements relating to their private life. Companies operating under US law can require employees to turn over company-related documents and data in their possession, comply with document hold and related directives.

In the European models (and other jurisdictions that have similar rules), the protection of an employee's privacy can be enforceable. The protection of privacy naturally finds one of its most important forms in the respect of the secrecy of private correspondence, including that sent by electronic means. At issue is the observance of fundamental rights and freedoms, including in the case of internal investigations: the right to privacy, respect for the privacy of home life and correspondence, freedom of expression and fairness in the finding of facts, among others.

The European Court of Human Rights (ECtHR) has developed case law attempting to balance the monitoring rights of the employer and the privacy rights of employees.[35]

In its *Barbulescu* ruling,[36] the ECHR provides a complete guide based on six questions to determine whether or not the employer has violated the employee's privacy protected by Article 8 of the European Convention on Human Rights. These questions must be asked to determine whether the employer can control the questionable element during an internal investigation:

- Has the employee been informed in advance of the monitoring carried out by the employer?
- What is the extent and degree of intrusion into the employee's private life?
- Is the employer able to justify one or more legitimate reasons for the monitoring of communications and access to the content of the messages?
- Were there less intrusive means of control than access to the content of the employee's communications?
- What were the consequences of the monitoring for the employee who was the subject of the monitoring?
- Was the employee offered adequate safeguards under national law?

This is a grid for analysis and hence a bundle of clues rather than questions that must be answered in an exhaustive manner.

As a principle, 'professional' emails and files can be reviewed and collected, even without the employee's consent (ie, work email account, files stored on a work computer or a USB key connected to a work computer, SMS and files stored on a work mobile phone, or documents stored in the workplace). The employer may, for example,

33 See, eg, *Uniformed Sanitation Men Ass'n v Comm'r of Sanitation of City of New York*, 426 F 2d 619, 626 (2d Cir 1970), explaining that although the choice between one's job and answering incriminating questions about on-the-job conduct 'may not be without pain, it is one that would confront an employee of a private company as a matter of course'.

34 *United States v Solomon*, 509 F 2d 863, 870 (2d Cir 1975); see also *Gilman v Marsh & McLennan Cos*, 826 F 3d 69, 74 (2d Cir 2016) ('No doctrine limits a company's inquiries as to allegations of employee misconduct.').

35 ECtHR, Grand Chamber, 17 October 2019, No 1874/13 and 8567/13, *Lopez Ribalda v Spain*; ECtHR, Grand Chamber, 5 September 2017, No 61496/08, *Barbulescu v Romania* ECtHR, 5th section, 22 February 2018, No 588/13, Libert v France.

36 *Barbulescu v Romania ECtHR*, Grand Chamber, 5 September 2017, No 61496/08, .

freely consult the business telephone records provided by the telecoms operator, even if the employees have not been informed in advance. On the other hand, most of the time it is impossible to review and collect 'personal' emails and files (ie, documents or emails that have been expressly identified as 'personal' or 'private' by the employee, or their personal email account, even if accessed from a work computer) without at least having previously informed the employee of such control.

Particular attention should be paid to the special case of protected employees (elected or unionised) who must be entirely free to fulfil their duties as elected officers or union members so the company does not run the risk of incurring charges of obstruction (in addition to the inadmissibility of such evidence – control is often impossible).

Given the complexity of the operations required and to avoid any further disputes, it is strongly recommended that companies call on an IT expert and a bailiff when carrying out such investigations.

Basic guidelines for companies when reviewing documents:

- Keep a clear record of who reviewed what and when.
- Ascertain where the documents are and who has access to them.
- Think about how to organise the collection of data and information.
- Consider how to individualise appropriate technology to be used.
- Determine the most efficient way of retrieving documents.
- Consider engaging forensic experts if necessary.
- Take some time to consider what level of review is proportionate in the circumstances (bearing in mind subsequent possibilities, such as litigation and regulatory investigations).
- Categorise documents by themes and relevance.
- Have a system for further review.
- Consider whether the investigation warrants putting documents onto a searchable electronic system.
- Once the documents have been retrieved, make an electronic back-up copy in case of a computer problem, but also have a blank copy of all the documents in case of subsequent legal proceedings.
- Remember to check the entire mailbox or basket looking for deleted emails or documents.
- Keep in mind the different disclosure requirements in different jurisdictions and anticipate any regulatory requirements for disclosing documents and requests for information.
- Think about whether the (permitted or tolerated) private use of a professional email account by the employee results in a restriction for the employer regarding the 'search' of the employee's email account or electronic folders.
- Assess whether privilege is maintained, especially in view of the different criteria in different jurisdictions.

Investigating individuals

As with for the document review, two radically different approaches exist when investigating individuals.

In many jurisdictions, monitoring employees, while perfectly acceptable because it is traditionally within the employer's power of direction and control, must nevertheless comply with the restrictions on exercising this power, related to the fundamental rights and freedoms of employees.

In other jurisdictions, such as the US, these problems are less likely to arise as the objective of accurate and complete fact-finding, which is the predicate for addressing improper or unlawful activity by company employees or third parties, is considered to be superior to the privacy of the employees. Indeed, the interest of the corporation and its shareholders tends to weigh more heavily than the privacy of its employees whose conduct may put the company at risk. Such employment arrangements generally grant companies broad powers to require that employees cooperate and make themselves available for interviews by authorised investigators. In many cases, companies can take adverse actions against employees for failures to cooperate in such activities, unless certain specific contexts (such as a whistleblower situation) apply. Even when employees invoke certain constitutional rights (eg, when the internal investigation is in fact attributable to public authorities who have outsourced their investigations to the company), such rights do not necessarily bar companies from disciplining employees for failure to cooperate.

Interviewing individuals

In many cases, verification of the facts makes it necessary to hold interviews.

Who should be interviewed?

To verify and process an internal report effectively, the company must proceed in a consistent manner.

It is often appropriate to first hear the person who reported a concern and ask for clarification or further information. Then, possibly and depending on the situation, the person or persons accused of being involved in the misconduct or wrongdoing should be interviewed.

Other people may be able to provide additional insight. This may be the case for employees who may be victims of the same acts or for employees who may have specific knowledge of the facts, such as accountants.

It may also be useful to ask the person who made the report and the person or people accused to propose a list of persons who could be heard in the course of the investigation (to corroborate their statements, testify to their personal experience or provide technical details).

Rules should also be made on whether the interviewees in the internal investigation have the right to be assisted during interviews. Since these are not disciplinary interviews, most jurisdictions do not recognise the right to be assisted, but it might nevertheless be appropriate to allow employees to be accompanied under certain conditions. The interviewers can at least inform the interviewee that they have the right to be assisted by a lawyer. However, the person may then believe that they are suspected, so the pros and cons have to be taken into account.

Interviews conducted by the company's lawyer

If an employee is interviewed by the company's lawyer, they must be told that the report on the interview is privileged not for their benefit but the company's (the 'Upjohn warning'). As a consequence, everything that the employee says can be disclosed if the company so wishes. When conducting an investigative interview, however, an attorney must ensure that the employee understands that the corporation, not the employee, is the attorney's client and that the corporation, not the employee, controls the privilege, including the decision about whether information gained during the employee's interview will be shared with third parties, including government regulators. This advice – called an Upjohn warning after a 1980 US Supreme Court case[37] – is

37 *Upjohn Co v United States*, 449 US 383 (1981).

critical both because it establishes the elements for a corporation's privilege claim and because it avoids a later claim that the communication established an attorney–client relationship with the employee. Not only can an incomplete Upjohn warning endanger the corporation's privilege claim, but it can also subject the attorney to ethics and disciplinary complaints for violation of the rules regarding conflicts of interest and duties of loyalty.

In some jurisdictions, the lawyer of the company who conducted the internal investigation cannot act in the employment litigation that may arise from the investigation.

The employer may also have an interest or a legal obligation to involve employee representatives in the investigation or even to ask them to attend the interviews.

Before the interview

The person in charge of the internal investigation must be provided with all relevant information concerning the 'whistleblowing internal report' and the documents provided by the person reporting the concern.

The purpose of interviewing the person who has reported misconduct or wrongdoing is to examine their situation and in particular to clarify their hierarchical position and functional role vis-à-vis the person(s) they are accusing or have named in the report.

Finally, the person in charge of the internal investigation must investigate the (initially summary) alleged facts to be able to ask relevant questions.

It is preferable not to prepare an exhaustive list of questions that must be absolutely asked because the questions will also depend on what the employee states.

The place and time chosen for the interview should also be considered. The interviewee needs to be in a comfortable environment. In particular, if there are several employees to be interviewed, it is preferable to ensure that they do not run into each other.

During the interview

The person in charge of the internal investigation must ensure that the interview takes place in conditions of strict confidentiality to ensure that the person reporting the misconduct or wrongdoing is protected.

It is also necessary to explain the context in which the interview is being held to the person being heard and then to alert the person reporting the concern and the employees being heard as witnesses that the procedure is confidential.

It is strongly recommended that neutral, factual and objective language is used when questioning to ensure the answers are not guided or distorted (voluntarily or otherwise).

The investigator may also inform the interviewee that they may ask for clarification if they do not understand a question. The investigator should also mention to the interviewee that they can take all the time needed to answer, to avoid giving incorrect answers. It is better to start by asking easy or obvious questions (about training, start date or professional background) to put the person more at ease but also note the person's body language to determine whether they are telling the truth.

The transition to the questioning must be gradual, starting from the general to the individual. Ideally, questions should be formulated in such a way that the person being interviewed can acknowledge the existence of the facts without necessarily feeling targeted, for example: 'Are you aware that such facts have occurred?'

Always conclude with a question like 'Has everything been said?' or 'Do you wish to add anything?'

The investigator should practise active listening to check that the information is understood correctly. The interviewer should not hesitate to rephrase if necessary.

After the interview

The person in charge of the internal investigation should write a report based on the detailed notes taken during the interview.

In the absence of legal rules governing interviews, it is often recommended that the report is proofread and countersigned by the person being interviewed. However, this may create a strong power balance in favour of the employer, which could have a negative impact on the employee. That is why getting the report countersigned by the interviewee should be assessed on a case-by-case basis. It is not recommended in the US jurisdiction.

In any case, the interview report should not be physically handed over to the employee to reduce the risk of leaks.

Identification of the person reporting the concern is indeed crucial: most judges cannot base their decisions solely or decisively on anonymous witness statements.

The signing of a formal non-disclosure agreement for all interviewees, setting out in particular the risk of potential criminal liability for breach of confidentiality, may sometimes be recommended.

Basic guidelines and questions for companies when interviewing individuals:

- Do not only interview those employees who have been accused; this could, in some jurisdictions, not constitute a real internal investigation.
- Do interview the employee accused in the report.
- The internal investigation should allow several employees to be heard, to avoid there being only one (unfair) statement of an employee in an individual conflict with the person accused in the report.
- Ideally several employees should be asked similar questions in order to enable objective comparison of the statements of each.
- It is essential in most jurisdictions to inform the employee that the interview has no connection with disciplinary proceedings.
- Do not communicate the results of the investigation to the employees who are interviewed, accused or victims; the consequences on the atmosphere among the company's employees must nevertheless be considered and the decision to carry out interviews must not be taken lightly.
- Conduct interviews with the help of at least two interviewers, for example, one asking the questions and the other taking notes.
- Prepare the questions with input from the relevant team members to ensure all perspectives are covered.
- Does an external labour lawyer need to be involved to review the wording of the questions before the interview?
- What are the requirements that the questions must meet to avoid being void? Consider issues of self-incrimination, discrimination, privacy, privilege, regulatory requirements, confidentiality and employee morale.
- What is the employer's legal position with regard to questioning employees? Do the employees have an obligation to answer? To what extent? Is the employee entitled to involve a lawyer or a member of the

works council or trade union representative? Does the principle of equality of arms apply?[38]

- How should employees' interviews be documented? Should they be recorded or written as reports and signed statements?
- Check whether the signature of the interviewee is required.
- Check whether there is need to give warnings about:
  - the right to use information against an individual;
  - limited expectations of confidentiality; and
  - the consequences of providing misleading or untruthful answers.
- Is there any need to involve a trade union, employee representative or works council? Consider rights and desirability of legal representation of individuals at meetings.
- Does the employer need to inform the internal data protection officer, or a governmental data privacy office?
- To what extent should the employee's right to privacy be respected? How should notifications or questions be posed to avoid the violation of this right?
- Are questions made in breach of the right to privacy valid? When can the right to privacy be waived?
- Ensure that interviewees do not come into contact with each other between interviews to ensure maximum confidentiality.

Temporarily excluding an employee

Provisional measures may also be adopted whenever the presence of the person to whom the complaint relates exposes other members of staff, and in particular the person reporting the concern, to the risk of retaliation.

The presence of the person to whom the complaint relates may create the risk of evidence being destroyed or concealed. For instance, in the case of harassment, for reasons related to the proper conduct of the internal investigation, it may be appropriate to exclude the alleged harasser or even the harassed employee.

In most jurisdictions, there is at least one labour law tool that can be used to exclude or remove an employee from the company during the internal investigation. These measures may be:

- suspension of the employee as a precautionary measure (eg, pending confirmation of dismissal);
- reassignment; or
- paid exemption from work.

The employee can be suspended as a precautionary measure, pending confirmation of dismissal, but this is always difficult because it implies in principle that disciplinary proceedings have begun. This therefore implies that the investigation is at a relatively advanced stage and that there is sufficient evidence to suggest the need for disciplinary action. It should be made clear that the suspension is a provisional measure (in the absence of specifying this, the suspension could be interpreted as a disciplinary layoff constituting, in itself, a sanction and depriving in some jurisdictions the employer of the possibility of dismissing the employee for the same facts).[39]

38 Ie, if the employer is represented by a lawyer, is the employee also entitled to be assisted by one?

39 Pursuant to the '*non bis in idem*' principle.

Finally, the implementation of provisional measures must be carried out with strict respect for the confidentiality of the proceedings, which can be very complex in practice.

Temporary reassignment can also be considered. However, the amendment of the contract must not last long and the measure taken must be temporary. The employer must act promptly – the measure is only valid as long as the needs of the investigation continue. Failing this, and because of the absence of concurrent disciplinary proceedings, there is considerable risk that the temporary reassignment may be reclassified by a judge as an illegal modification of the employment contract or as a disciplinary sanction preventing the offending employee from subsequently being dismissed.

As a corollary to remuneration, the employer's first obligation is to provide work for its employee. Paid exemption from work consists in temporarily suspending by mutual agreement the obligation of the employer to provide work for its employee and, correlatively, the employee's obligation to work, without affecting their remuneration. Such a measure must generally be taken with the consent of the employee because it implies the suspension (and therefore a modification) of the employment contract. This measure may be useful in temporarily removing an employee with whom the employer maintains a good relationship. This may be an employee who is or feels a victim of harassment, especially when the employee is not on sick leave.

Naturally, these difficulties do not arise in jurisdictions where 'employment at will' prevails, since the employer does not necessarily have to justify not giving work to the employee.

Tracking an employee

Given that 95 per cent of perpetrators are 'proactive' and take steps to conceal their actions,[40] the internal investigations of individuals by interviews may not be sufficient to gather evidence.

For example, in the most insidious cases of harassment, the perpetrator not only takes care not to leave any written record of their actions, but also carefully acts out of the view of others, so that interviews and checking emails or files are ineffective.

Surveillance of the employee outside work time and the workplace rarely seems justified or proportionate to the objectives pursued. Under French law, for example, it is not only the home that is protected; privacy also extends to travel in public spaces, such as the street.

In principle, any recording made without the employee's knowledge is prohibited. This also applies to video recordings made at the premises of a client company, and to wiretaps or recordings of telephone conversations. Any scheme aimed at confusing employees is also prohibited. It should be remembered that although the use of a bailiff does not in itself constitute an unfair method of obtaining proof, it becomes so if the bailiff conceals their status from the employee concerned or stages a situation to cause the person concerned to commit wrongdoing.

Using a private investigator might be appropriate in the case of remote locations, sensitive personal issues or technical or forensic expert knowledge. However, private investigators may not be sensitised to how their tactics will be perceived by judges, regul2tory authorities or the public, which could create legal and reputational risks for the company.

When using a private detective the following precautions apply:

- Private investigators should preferably be retained by outside counsel.
- Do a strict conflict check and non-disclosure agreement.
- Give clear instructions about the scope of the investigation and the fact that only legal means may be used

40 See n 6 above.

to obtain evidence.

- Careful supervision is necessary.
- Discourage or even prohibit the use of sub-contractors.

The introduction of measures to organise the tracking of employees outside the company, using a private detective, or recording or wiretapping individuals must systematically be preceded by the advice of a lawyer from the local jurisdiction. Indeed, in many jurisdictions these cannot be done without a judge's prior authorisation.

What Happens At The End Of An Internal Investigation?

Record or disclose the investigation

When the investigation is completed and the company has been able to confirm the accuracy of the facts investigated, the question of what to do with this information arises.

Although it seems obvious to keep a record of the internal investigation, the issue of disclosure of information must be carefully examined, especially since most of the rules protecting personal data will still apply at this stage.

There could also be another practical issue related to confidentiality that is psychological. For example, in the case of a harasser who is dismissed after a whistleblowing report (or transferred or reassigned to another service) without any particular publicity, the victim could be left with a deep sense of dissatisfaction because the perpetrator is only informally 'sanctioned'. Special attention should be paid to this situation as it may lead the victim to public disclosure even though the case has been dealt with and resolved internally.

In the event of an investigation before potential prosecution by the authorities, depending on the jurisdiction, companies either: (1) voluntarily disclose the facts to the authorities, to possibly benefit from a 'deferred prosecution agreement' (judicial agreement in the public interest); or (2) sanction internally without informing the authorities.

In the latter case, the company must be able to justify in due course: (1) that it implemented all necessary sanctions; and (2) it prevented the repetition of these acts through corrective measures.

Under the jurisdiction of the US, it is not uncommon for corporations that have discovered violations of law in the company, through an internal investigation or otherwise, to disclose such wrongdoing to enforcement agencies.

The willingness of US companies to make voluntary disclosures and to cooperate with enforcement agencies is spurred by several factors:

- the long odds of successfully challenging the broad subpoena power of government agencies;
- the fact that US corporations have no constitutional right to withhold documents on the grounds that they would be self-incriminatory;
- the doctrine of '*respondeat superior*', under which a company itself may be held liable for the acts of its employees; and
- most recently, government policies indicating that the authorities may decline to prosecute if a company has voluntarily disclosed and fully cooperated.

Whether to make a voluntary disclosure of wrongdoing nonetheless presents a tactical decision for companies. Disclosure may mitigate fines and penalties or even avoid liability entirely.

However, the downsides of disclosure include increased costs, the possibility of a follow-on government investigation and exposure to penalties. Thus, most companies subject to US jurisdiction evaluate their options on a case-by-case basis to determine what steps would be in the best interests of the company.

Basic guidelines for companies when closing the file:

- Check whether the findings of previous investigations may be used in an ongoing one, or vice versa.
- Determine the list of people who must be informed of what in relation to the findings of the investigation

(both internally and externally, including regulators and other authorities).

- Consider the possibility that not all findings need to be communicated to all parties involved.
- In the case of disclosure, consider how findings should be disclosed. Depending on the aim of the investigation, lawyers usually write a privileged report on the facts, but qualify the said facts orally only to avoid their findings being seized. Another way of preventing the findings from being disseminated is to avoid sending anything by email so that no one transfers it, but to circulate only hard copies.
- Assess if the findings are an efficient evidence tool.

Evidential value of the investigation report

The internal investigation report will become a key piece of evidence before the judge. Although it would be excessive to claim that its probative value is uncertain, it must be noted that it varies enormously according to the different cases and jurisdictions in question.

Indeed, as evidence and facts, the evidentiary value of the internal investigation is left to the discretion of the judges. An internal investigation that is conducted by the employer unilaterally, biased and unfairly is likely to be excluded from the judicial proceedings. The fact that an internal investigation has concluded that the allegations were not proven does not bind the court.

In France, for example, a general requirement of good faith implies discretion, impartiality and fair treatment during the establishment of the internal investigation report. The purpose of complying with such obligations is to make the investigation sufficiently serious and credible in the eyes of the judge.

According to established French case law, a real and serious cause of dismissal cannot be essentially based on an anonymous witness statement. The French Court of Cassation had the opportunity to reiterate this principle in a judgment of 4 July 2018: 'the judge may not base his decision solely or decisively on anonymous witness statements'. This principle is adopted in most jurisdictions. However, this is naturally not a concern in jurisdictions where 'employment at will' prevails, such as in the US.

In a judgment of 19 June 2018, the Criminal Division of the French Court of Cassation had to rule on the traditional technique of hearing witnesses, which consisted of taking note of the remarks of the employee interviewed without citing them verbatim. The Criminal Division considered that 'the transcript of the statements made by witnesses heard during the internal investigation cannot constitute a forged intellectual, as these witnesses, to whom the transcript of their statements had been given, had not requested corrections'. Two lessons can be drawn from this:

- the countersignature of the interview reports by the employee remains recommended practice; and
- the absence of a countersignature is not a decisive factor if the employee has not requested changes to the final text, as long as it is possible to determine the identity of the employee who made the statement.

Data retention rules and privacy

Data protection requires many precautions. Whether it is to keep the data in a safe place or to archive it later, several good practices common to all jurisdictions can be provided:

- Use secure means of communication in the context of exchanges between persons (especially the compliance officer and the person in charge of the investigation) by, for example:
  - recording the facts, stages of the investigation and the interview reports;

  - password-protecting files rather than summarising the content in the body of an email; and
  - ensuring that the email cannot be transferred.
- Remind all persons involved that it may be preferable:
  - not to print the documents drawn up as part of the investigation, such as interview reports; or
  - if they are printed, to keep them locked away and not accessible to other employees; or
  - to destroy the documents as soon as possible.

Outcomes of the internal investigation

The closure of the investigation requires the preparation of an investigation report. At the end of the investigation, the investigator draws up a report in which they record:

- the conditions under which and date the matter was referred to them;
- the facts revealed by the person who reported the misconduct or wrongdoing and the evidence provided in support of their allegations;
- the duration of the investigations and the acts of investigation carried out (eg, number and identity of persons heard, and verifications carried out);
- the investigator's conclusions as to the veracity of the facts reported; and
- the action they suggest should be taken.

Always check if some follow-up actions after the investigation are necessary.

In a disciplinary context, companies need to be mindful of the existence of a period of limitations to sanction an employee. In theory, if there is an investigation, this period does not begin until the investigation is complete, unless the employer intentionally conducted unneeded investigations for the purpose of getting around the period of limitation.

In a contractual or commercial framework, the follow-up action would be to terminate contractual or commercial relations with third parties whose fraudulent or unfair involvement is proven by the internal investigation.

In a judicial context, analyse the situation to determine whether there is an obligation or opportunity to file a suit (if the company is a victim of the facts investigated) or to report or disclose the facts.

Conclusion: Ten-point Checklist

1. **Ensure** the credibility of the allegations and the source before starting an internal investigation.
2. **Understand** the nature and scope of the internal investigation.
3. **Appoint** investigators according to the nature of the internal investigation.
4. **Manage** communication and organisation and take protective measures if necessary.
5. **Collect** and review documents.
6. **Interview** the employees involved or other witnesses and take interview notes.
7. **Decide** and communicate (or not) on corrective measures and sanctions.
8. **Draft** the final report.
9. **Consider** any useful action to be taken as a result of the internal investigations (protecting the victim, witnesses and whistleblower; breaching contracts; taking legal action; sanctioning an employee; or disclosure to public authorities).
10. **Archive** the file or ensure its lawful preservation.

Appendix: Internal Investigations And Impact Of Legal Privilege's Different Conceptions[41]

Definition of legal privilege

Canada

Although the law on privilege varies across Canadian jurisdictions, generally speaking, there are three forms of privilege: (1) solicitor–client privilege; (2) settlement privilege; and (3) litigation privilege. Set out below are certain rules governing the applicability of solicitor–client privilege to investigations in most Canadian jurisdictions.

Solicitor–client privilege prevents disclosure of information communicated to a lawyer for the purpose of obtaining legal advice. There are three key elements needed for a communication to be protected by solicitor–client privilege:

1. the communication was between a solicitor and a client;
2. the communication entailed the seeking or receiving of legal advice; and
3. the client intended the communication to be confidential.

England and Wales

Privilege entitles a party to refuse to disclose certain confidential legal communications to third parties, including courts and investigating authorities. There are two main types of privilege: legal advice privilege and litigation privilege.

Legal privilege advice applies only to communications between a lawyer and their client. The communication must be with a lawyer (not other professional advisers). This includes foreign lawyers.

The 'client' is the person or group of people within the client company who has been given responsibility for obtaining legal advice; not all employees of a client will be clients for the purposes of privilege.[42]

In practice, this means that communications between a lawyer who is carrying out an investigation and witnesses who might have evidence relevant to the investigation will not be covered by legal advice privilege, even if those witnesses are employees of the client company. The communication must be (and remain) confidential. The communication must be for the purpose of giving or obtaining legal advice, which includes what should be done more broadly in the relevant legal context.

Litigation privilege applies to communications between a lawyer and their client, or either of them and a third party (which will include, eg, witnesses, experts and other professional advisers). The communication must be for the dominant purpose of litigation or adversarial proceedings, where those proceedings are existing, pending or reasonably in prospect.[43] Litigation privilege may apply in the context of an investigation provided that the investigation is sufficiently adversarial in nature.[44]

Determining whether litigation privilege applies in an investigation's context is fact-specific and can be difficult. It will often not apply in the early stages of an investigation when the full facts will probably not be known. It may

41 Although the information provided is accurate as of September 2019, be advised that this is a developing area.

42 *Three Rivers District Council and others v The Governor and Company of the Bank of England* (No 5) [2003] QB 1156 CA.

43 *Three Rivers District Council and others v The Governor and Company of the Bank of England* (No 6) [2005] 1 AC 610 (HL) at 102; *Wheeler v Le Marchant* (1881) 17 Ch D 675, at 680-1.

44 *Serious Fraud Office v Eurasian Natural Resources Corporation Ltd* [2018] EWCA Civ 2006.

be that litigation privilege does not apply when an investigation starts but that, as it progresses, facts emerge that mean litigation is reasonably in prospect.

France

Confidentiality is a fundamental rule by which French lawyers are bound. It is general, absolute and unlimited in time. It is a public policy measure that protects both the private interests of the client and general public interest.

It has been implemented by Article 66-5 of the Law dated 31 December 1971 and Article 4 of Government Order No 2005-790, dated 12 July 2005.

Confidentiality resulting from the duty of professional secrecy applicable to external counsel applies to any matter brought to the lawyer's attention in exercising their profession. Violation by a lawyer of the duty of professional secrecy is punishable by criminal and disciplinary sanctions.

Although professional secrecy is a duty for the lawyer, it also allows a lawyer to benefit from a protective regime (inviolability of the lawyer's premises, confidentiality of correspondence and telephone conversations). This protection ceases if the lawyer is suspected of having participated in an offence.

A lawyer cannot be compelled to testify in a case involving a client. A lawyer cannot share privileged information or information subject to legal privilege with anyone, except members of their firm and president of the Bar.

No waiver of secrecy is possible under French law: the lawyer cannot waive it even with the agreement of a client.

Germany

Attorneys operating in Germany have a professional duty of confidentiality. This means that any information they acquire while exercising their profession must remain confidential. Any breach of this duty can constitute a crime according to section 203(1)(3) or section 204(1) of the German Criminal Code (Strafgesetzbuch). Attorneys can only be released from their duty of confidentiality by their clients. In fact, there are only a few exemptions from the duty of confidentiality, for example, if the attorney is under investigation because of the advice given to the client and needs to defend themselves.

A German attorney's professional duty of confidentiality corresponds to the attorney's right, indeed obligation, to refuse testimony in court both in civil cases, according to section 383(1)(6) of the Civil Procedural Code (Zivilprozessordnung), and in criminal cases, according to section 53(1)(3) of the Criminal Procedural Code (Strafprozessordnung). In fulfilling a mandate, the right of attorneys to refuse testimony concerning any information obtained in execution of their profession is further strengthened by protection against seizure of potential evidence under certain circumstances. While the limits of this protection need further clarification by German courts, the core requirements according to sections 97 and 148 of the Criminal Procedural Code are defined as follows:

- Only written communications between the attorney and the client under suspicion (Beschuldigter) are protected by privilege, including any mandate-related work produced by the attorney, for example, notes, memos and draft statements.
- Protection against seizure is only granted if the respective documents are in the possession of the attorney.
- If the attorney's mandate and the corresponding communication or work produced by the attorney or client concern criminal legal defence, protection against seizure is granted whether the said documents are in the possession of the attorney or the client. This distinction is based on the content of the documents, not on the explicit use of the term 'communication for defence purposes' (Verteidigerkorrespondenz).

Malaysia

Legal professional privilege in Malaysia is provided for under legislation and common law.

The legislative basis for legal professional privilege is provided for in Articles 126 to 129 of the Evidence Act 1950. Article 126 applies to advocates and prohibits them from disclosing communications, documents or advice given by them to their client unless they have their client's express consent, subject to the exceptions therein. Article 129 states that no one shall be compelled to disclose in court any confidential communication between them and their legal professional adviser.

Malaysian common law also recognises litigation privilege, which operates to cover documents produced or information collected for the sole purpose of pending or anticipated litigation (*Dr Pritam Singh v Yap Hong Choon* [2007] 1 MLJ 31). Recently, however, the existence and operation of litigation privilege has been called into question by two conflicting Court of Appeal decisions:

- *Tenaga Nasional Bhd v Bukit Lenang Development Sdn Bhd* [2016] 5 MLJ 127, which held that the law relating to privilege was codified and as such restricted by the Evidence Act; and
- the subsequent case of *Wang Han Lin & Ors v HSBC Bank Malaysia Berhad* [2017] MLJU 1075, which appears to have restored the recognition of litigation privilege in Malaysia, and stated that the test for determining whether litigation privilege may be successfully established is as follows:
  - Is litigation pending or apprehended? In other words, is litigation reasonable in prospect?
  - Is litigation the dominant purpose for which the report was prepared?

US

In the US, the attorney–client privilege is a creature of federal and state laws, and so the definition may differ somewhat depending on the particular court that is considering the issue and whether the matter involves federal or state law.

However, in general the attorney–client privilege will protect the confidentiality of communications where:

- the person asserting the privilege is or sought to become a client;
- the person to whom a communication was made is an attorney (or agent of an attorney) acting in their legal capacity;
- the statement was made in confidence, outside the presence of any third party, for the purpose of securing legal advice and not for the purpose of committing a criminal act or tort; and
- the privilege has been claimed and not waived by the client.

The purpose of the privilege is to foster open communications between client and attorney so as to promote compliance with the law.[45] In addition, the 'privilege recognizes that sound legal advice or advocacy serves public ends' and the administration of justice and 'that such advice or advocacy depends upon the lawyer being fully informed by the client'.[46] The attorney–client privilege in the US is also a creature of the rules of discovery and evidence. The reason its preservation is often first and foremost on the mind of a lawyer advising a client is because of the breadth of US discovery. These rules may require the disclosure to an adversary in a litigation of 'any nonprivileged matter that is relevant to any party's claim or defense'.[47] The all-encompassing nature of US

45 See *Upjohn Co v United States*, 449 US 383, 389 (1981).

46 *Ibid.*

47 Rule 26(b)(1) of the Federal Rules of Civil Procedure provides: 'Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs

discovery creates a risk that, in the event the attorney – client privilege is not properly preserved or is waived, a party will be ordered to disclose communications between client and counsel to an adversary.

It is important to recognise that the attorney–client privilege in the US is fundamentally very different from, and broader than, what is often recognised in other jurisdictions. The privilege in the US does not merely reflect an obligation or duty on counsel not to disclose information received from the client. In the US, in most instances, neither a lawyer nor a client may be required to testify, whether at trial or in a deposition, or even in an investigation, about privileged communications; nor may lawyer or client be compelled to produce privileged communications.

The privilege survives the end of the attorney–client relationship. The privilege protects from disclosure to any party, including the government, all communications between counsel and client. Thus, neither the client (or potential client) nor counsel may be compelled by any entity to disclose this information, so long as the privilege is not waived.

The issue of waiver is complex and goes beyond the scope of this brief article. Waiver may be intentional or unintentional. The privilege belongs to the client, not the lawyer. Waiver may occur in the following circumstances:

- the communication was made in the presence of individuals who were neither attorney nor client, or was disclosed to such individuals;
- the communication was made for the purpose of committing a crime or tort; and
- the client has waived the privilege (eg, by publicly disclosing the communication, or by disclosing the information in a litigation, inadvertently or otherwise).

However, waiver may be avoided in some circumstances. For example, federal law recognises a limited exception, known as the Kovel[48] or 'derivative' privilege, when disclosure to a third party, such as an expert accountant, or other expert, is necessary to facilitate attorney–client communication.

Rule 502(b) of the Federal Rules of Evidence also permits the parties to litigation to preserve the privilege if there has been an inadvertent disclosure in the course of discovery. Thus, when the disclosure is made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in that proceeding if:

- disclosure was inadvertent;
- the privilege-holder took reasonable steps to prevent disclosure; and
- the privilege-holder took prompt reasonable steps to retrieve the documents upon discovering the error, including (if applicable) after Fed R Civ P 26(b)(5)(B).

Is a lawyer allowed to conduct an internal investigation in a company?

England and Wales

It is common for lawyers to conduct internal investigations in a company.

of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.'

48 The Kovel doctrine, set forth in *United States v Kovel*, 296 F 2d 918 (2d Cir 1961), describes the parameters for the extension of the attorney–client privilege to non-attorney third parties.

France

In France, as in most European jurisdictions, a lawyer can investigate on behalf of a company, but under strict conditions.

After a recent study on the lawyer in charge of an internal investigation, the Paris Bar Council added an Annex XXIV to the Parisian internal regulations of the legal profession, by a decision dated 8 March 2016.

After some debate, the Paris Bar Association confirmed in 2019 that lawyers may conduct internal investigations for a company that is their client and that the internal investigation would, in principle, be covered by legal privilege.[49]

More precisely, the Paris Bar Council considers that an internal investigation falls within the professional scope of the lawyer.

There are general recommendations for the lawyer in charge of investigating on behalf of a company:

- The lawyer in charge of an internal investigation must observe, in all circumstances, the essential principles attached to the practice of the legal profession, in particular, the principles of conscience, independence, humanity, loyalty, moderation, competence and prudence. They must refrain from placing any pressure on the persons being heard.
- The lawyer should conclude an agreement with the client or the persons appointing them, which, in addition to the terms of the lawyer's remuneration, will define the purpose of their assignment.
- As in all matters, the lawyer in charge of an internal investigation is bound by privilege with respect to their client alone. No one else may solicit the benefit of such privilege. In accordance with the rules of professional secrecy, when a report or other document is drawn up by the lawyer during their mission, it is given exclusively to the client, who remains free to disclose it to a third party.
- Before any contact with third parties or employees for the purpose of carrying out the internal investigation, it is imperative that the lawyer explain their mission and its non-coercive nature. The lawyer must specify that exchanges are not covered by professional secrecy with regard to them and that the comments made may be transcribed in whole or in part in their report.
- The lawyer in charge of an internal investigation in the context of assistance or advice may be the client's usual lawyer or a lawyer who has never worked for that client before. However, the lawyer in charge of an internal investigation may not accept an investigation that would lead them to make an assessment of work that they have previously carried out.
- In all circumstances, the lawyer must mention to the people they interview during the internal investigation that they are not their lawyer but are acting on behalf of the client who has appointed them to carry out the investigation.
- The lawyer shall explain to the people interviewed or contacted for the purposes of the internal investigation that the privilege owed to their client is not binding on the latter, so that the statements and any other information gathered during the investigation may be used by the client, as well as the report submitted to the client, if any.
- The lawyer shall inform the person being interviewed that they may be assisted or advised by a lawyer when it appears, before or during the hearing, that they may be accused of an alleged wrongdoing as a result of the internal investigation.

49 See n 31 above.

- The lawyer may assist their client in a procedure, whether amicable or contentious, relating to or following the internal investigation, but shall refrain, in particular because of the principle of delicacy, from representing the client in a procedure directed by the latter against a person whom the lawyer has interviewed during the internal investigation.
- The lawyer in charge of an internal investigation will have to ensure their independence with respect to the management of the investigation and possible exchanges with a public authority. If their independence might be compromised, the lawyer in charge of an internal investigation shall recommend to the client to be represented by another lawyer for the separate stages of the internal investigation.

Germany

According to German law there are no restrictions on attorneys conducting internal investigations in a company. The question that needs to be addressed vis-à-vis general permission to conduct internal investigations is whether work produced by the attorney concerning the investigation, for example, interview memos or reports, is protected against seizure.

Italy

Internal investigations are gradually becoming common practice in Italy, at least for large business organisations, either as an instrument of the internal control system to manage red flags of potential misconducts (such as whistleblower allegations) or as a reaction to criminal investigations started by public prosecutors.

Companies may decide to delegate the conduct of the investigation to a corporate function, usually internal audit or compliance. Even where in-house lawyers are involved, however, these kinds of internal investigations are not covered by legal privilege. They actually constitute a remedial action usually expected to be presented to the acting prosecutors or to the competent judge to prevent application of interim measures or to mitigate sanctions.

Companies may also decide to appoint an external counsel to conduct the internal investigation. This is common practice when criminal proceedings have been initiated, when legal privilege must be preserved or when independent legal advice is particularly needed. In these cases, the best practice to secure legal privilege to the maximum extent allowed by the law is to appoint the external attorney with the formalities provided under Italian law for the so-called defensive investigation.

The Italian Code of Criminal Procedure (ICCP) expressly regulates the 'defensive investigations', for the performance of which any private party to criminal proceedings – the person under investigation or defendant, the offended party, or the other parties civilly liable for the offence – can formally engage a defence attorney (Article 327-bis, ICCP). In the absence of pending criminal investigation, the law also allows private parties to engage an attorney to conduct the so-called preventive defensive investigation, that is, investigations conducted in anticipation of the possibility that such criminal proceedings are initiated by public prosecutors (Article 391-*nonies*, ICCP).

Since companies can be or became party to criminal proceedings – in particular, entities can be held liable for certain criminal offences committed by their directors, managers, employees or agents pursuant to Legislative Decree No 231/2001 – they are therefore entitled to engage an external attorney to conduct defensive investigations, also in the form of preventive defensive investigation.

The attorney appointed as defence lawyer for the conduct of defensive investigations can delegate the performance of certain activities to a substitute attorney, licensed private investigators or expert consultants (Article 327-bis, par 3, ICCP).

The conduct of defensive investigations is regulated by: (1) Articles 391-bis et seq and other special provisions of the ICCP; (2) Article 55 of the Lawyers' Professional Code of Conduct; and (3) the Rules of Conduct of Criminal Lawyers in the conduct of defensive investigations (the latter was approved by the organisation of criminal attorneys Camere Penali and binds only its affiliates).

The Netherlands

Lawyers are permitted to conduct investigations into a wide variety of topics. There are no specific rules applicable to internal investigations by lawyers, other than those resulting from the professional rules of conduct applicable to all lawyers admitted to the bar.

US

There is no ethical restriction on an attorney conducting an internal investigation in a company, and indeed, attorneys are often called upon to do so.

Does legal privilege apply to the findings of the internal investigation?

Canada

With respect to investigations, since solicitor–client privilege only arises where a lawyer is giving legal advice to a client, privilege would not protect communications related to an investigation where the lawyer is acting solely as an investigator. However, if a lawyer is conducting an investigation for the purpose of giving legal advice to a client, solicitor–client privilege would attach to the communications between lawyer and client (the investigation report), as well as the investigating attorney's notes.

Where an investigation is privileged, privilege would also attach to the factual sections contained in an investigation report (and to the investigator's notes), to the extent that these are inextricably linked to the legal advice to be provided. However, privilege only protects lawyer–client communications, not the underlying facts.

England and Wales

Not always. The law of privilege is complex and much depends on the particular facts. Legal advice should be sought when planning the scope, objectives and structure of an investigation so the extent of privilege protection can be determined.

France

As a principle, legal privilege applies when a lawyer conducts an internal investigation on behalf of its client.

When legal privilege applies, it covers all the elements of the file, including the internal investigation report, and:

- correspondence exchanged between the lawyer and their client;
- correspondence between lawyers, with the exception of those marked 'official' (ie, correspondence which relates to procedural documents or which makes no reference to any confidential prior written material, comments or elements);
- consultations addressed by the lawyer to their client relating to the strategy to adopt for the internal investigation;

- interview notes, but only between the lawyer and their client (not for the benefit of the persons being interviewed);
- file documents;
- information and confidences; and
- lawyer's agenda.

Professional secrecy applies whether the medium is tangible or intangible (eg, telephone, fax or email).

Germany

It depends. Protection against seizure as described above applies when the requirements according to sections 97 and 148 of the Criminal Procedural Code are met.

In its so-called Jones Day decisions dating from 27 June 2018[50], the Constitutional Court has clarified that there is no breach of any constitutional rights of Volkswagen AG by the German criminal courts requiring that an attorney–client relationship and a position analogous to a 'suspect' (beschuldigtenähnliche Stellung) are mandatory for any protection against seizure. The respective criminal courts were of the opinion that if a company is the client, the attorney–client relationship needs to be established between the attorney and the company under suspicion. Any protection against seizure granted with regard to the parent company of a group of companies does not automatically apply to any subsidiary companies.

The facts upon which the Jones Day decisions are based are as follows:

- In the course of the analysis of the so-called "diesel scandal", Volkswagen AG hired the law firm Jones Day in September 2015 in order to conduct an internal investigation to clarify the facts regarding any irregularities discovered with regard to the diesel engines in question. Jones Day conducted a group-wide investigation and Audi AG had agreed to Jones Day conducting the investigation within its operations without having appointed Jones Day itself.
- Because of these irregularities, the public prosecutor's office in Braunschweig started an investigation in September 2015 against those individuals at VW AG who were allegedly responsible and against VW AG in April 2016.
- At the beginning of March 2017 the public prosecutor's office in Munich initiated a similar investigation against individuals at Audi AG, which was extended to include Audi AG in June 2017,. In March 2017 the appointed public prosecutor in Munich searched Jones Day's office in Munich and secured 185 binders of documents and electronic data – all material related to the corresponding internal investigations. The documents were secured because the prosecutor wanted to examine them in order to determine which of them needed to be formally seized as they were possibly relevant for the criminal proceedings.

Since the attorney–client relationship was established solely between Jones Day and Volkswagen AG and not with Audi AG, the material pertaining to the internal investigation conducted by Jones Day was not protected against seizure in the corresponding criminal proceedings conducted by the public prosecutor in Munich against Audi AG. Volkswagen AG was under investigation in the proceedings conducted by the public prosecutor in Braunschweig but not in the proceedings conducted by the public prosecutor in Munich.

Another important aspect of the Jones Day decisions is that the Constitutional Court had no constitutional doubts regarding the opinion of the criminal courts on the moment defining the beginning of protection against seizure:

50 German Constitutional Court, 27 June 2018, No 2 BvR 1405/17, No 2 BvR 1780/17, No 2 BvR 1562/17, No 2 BvR 1287/17, No 2 BvR 1583/17.

- In cases in which a company merely 'fears' that an investigation against the company could be initiated and therefore seeks criminal legal advice or starts an internal investigation, no such protection would need to be granted.
- The protection against seizure shall require more than simply a 'fear', but less than a formal position of the company as a 'suspect' in the corresponding proceedings. What is required is a probability that a corporate representative has committed a crime or has not fulfilled a duty of supervision, which can lead to a corporate fine.

It is therefore possible that protection against seizure is not granted if an internal investigation is conducted at a very early stage even though all the other requirements are met and irrespective of any civil legal duty of the company's management to clear up any offences. However, further developments, especially at the legislative level, need to be observed closely.

Italy

Confidentiality of the findings of defensive investigations conducted by a formally appointed external attorney constitutes both a duty of the attorney and a legal privilege, ensured by different layers of protection.

No obligation to file the findings of the defensive investigation with the competent judge, or to report crimes

The defence attorney may decide to disclose to the judge the findings of their defensive investigation, in which case the material is included in the defence records and will be taken into account by the judge competent for the decision on the matter. This is a discretionary decision, meaning that the attorney has no duty to disclose any of the evidence collected in the investigation, nor is under any obligation to report to the public authorities any criminal violations that they may have become aware of in the performance of their engagement.

Duty of confidentiality of the attorney (scope of the 'professional secrecy')

Pursuant to the law regulating the legal profession (Article 6, Law 247/2012) and to the Lawyers' Professional Code of Conduct (Articles 13 and 28), Italian attorneys are obliged to maintain confidentiality and the so-called professional secrecy over all facts and information relating to their clients that they have learnt from any source during the performance of their judicial or extrajudicial functions, or in any event for professional reasons. The Professional Code of Conduct also provides for the specific duty of secrecy over any act of the defensive investigation and its content (Article 55, para 3). The violation of such duty of professional secrecy is grounds for disciplinary sanctions enforced by the Italian Bar, and can be a cause for civil liability to the extent that it caused damage to any party.

Under Article 622 of the Criminal Code, revealing a professional secret without just cause or using it for the profit of oneself or a third party, and thereby procuring potential damage, constitutes a criminal offence that can be prosecuted upon request of the harmed person (normally, the client).

Legal privilege covering professional secrets

Under Articles 200 and 256 of the ICCP (and Articles 118 and 249 of the Code of Civil Procedure), attorneys and licensed private investigators or expert consultants acting at their direction:

- cannot be compelled to testify about the information that they have known in the performance of their profession; and
- can refuse to hand over documents and other electronic data in their possession requested by judicial authorities, by opposing in writing that such documents are protected by professional secrecy. The judge

has the authority to verify whether the opposition of the professional secrecy is grounded.

- Under Article 197 of the ICCP, the defence attorney who conducted defensive investigation cannot in any case stand as witness in the criminal proceeding in relation to which the defensive investigation has been performed.

Enhanced privilege for defence attorneys, including investigating attorneys (attorney-client communications)

Under Article 103 of the ICCP, public prosecutors:

1. cannot wiretap conversations and communications between the defence attorney, licensed private investigators or expert consultant, or between them and the client;

2. cannot seize any document related to subject of the defence or investigations in the possession of attorneys, or of appointed licensed private investigators or expert consultants;

3. cannot carry out inspections and searches of the defence attorney's premises, unless the defence attorney is themselves charged with a crime or to find specific persons or items that have been specifically identified (in such cases, the inspection must be carried out by a judge or by the public prosecutor authorised by the judge, and must be previously notified to the local Bar so that a representative of the Bar can be present); and

4. cannot seize or control any correspondence between the attorney and the defendant or investigated person, unless the judicial authorities have grounded reasons to believe they constitute *corpus delicti* (ie, items upon which, or by which, the crime has been committed, or items that are the product, profit or price of the crime). Correspondence must be labelled '*corrispondenza per ragioni di giustizia*' and must show client's name, lawyer's name and qualification, signature of the sender and reference to the criminal proceedings.

Rules mentioned under the first three points apply to defensive investigations even in the form of a preventive defensive investigation. The fourth point also applies, in our opinion, to preventive defensive investigation; however, as far as we are aware, this interpretation has not been tested in courts yet.

The aforementioned confidentiality and secrecy rules concern information exchanged with, or learned by, independent external attorneys and their staff for the purpose of legal advice.

Malaysia

It is possible that legal professional privilege may be invoked on the findings of internal investigations under certain circumstances that fulfil the articles of the Evidence Act or the requirements for litigation privilege. This would depend on, among other things: the purpose of the investigation; the party responsible for conducting the investigation and preparing the report or the party who called the report into existence; to whom the relevant findings or reports have been communicated; and from whom disclosure of the report is being sought. However, as stated later, there are further limitations to the scope of legal professional privilege.

The Netherlands

The prevailing view is that legal privilege attaches to the findings of internal investigations. There is, however, some debate as to whether privilege indeed applies. This follows mostly from a court decision in which the court held that an internal investigation report produced by lawyers that merely contains factual information is not covered by privilege. The decision seems to be influenced by several additional circumstances particular to that case, and was widely criticised. Nevertheless, there remains debate as to whether investigative reports that merely contain factual information are covered by privilege.

US

If the investigation is conducted for the purpose of obtaining legal advice, then the company may expect that the investigation and results will be privileged and confidential. However, if the content of an attorney investigation is substantially at issue in litigation, the privilege may be lost.

In *Brownell v Roadway Package System*,[51] the plaintiff sought to obtain statements given by her former employer to its counsel before her termination. The statements were elicited from the defendant's employees during the course of the defendant's investigation into the plaintiff's sexual harassment allegations. The Court held that because the defendant raised the affirmative defence of adequate investigation and prompt responsive action, it had waived the attorney–client privilege and must disclose the reports.[52] Where 'an employer relies on an internal investigation and subsequent corrective action for its defense, it has placed that conduct "in issue" [… and] may not prevent discovery of such an investigation based on attorney-client or work-product privileges solely because the employer has hired attorneys to conduct its investigation'.[53]

In *Pray v New York City Ballet Co*, the magistrate judge granted the plaintiff's motion to compel the depositions of outside counsel regarding communications between the ballet company and its counsel: (1) during the investigation; (2) for the purpose of initiating the investigation; and (3) after the investigation concluded. The district court reversed the decision in part, holding that the initial and post-investigation communications were protected by the attorney–client privilege.[54] Thus, even if the investigation materials lose their privileged status because of assertion of an affirmative defence, the employer may still be able to assert privilege as to its advice concerning the results of the investigation.

Does it apply regardless of who is in charge of the investigation (lawyer, in-house counsel, other)?

Canada

Privilege would not apply to internal investigations conducted by individuals who are not attorneys. Privilege may apply to an internal investigation conducted by an in-house attorney, depending on whether the attorney was acting as counsel and providing legal advice. This is determined through a case-by-case factual analysis.

England and Wales

The type of privilege (either legal advice privilege or litigation privilege) that will apply will depend on the circumstances and purpose of the investigation; for example, if the aim of the investigation is to provide legal advice, or if adversarial proceedings are in reasonable contemplation.

In the context of legal advice privilege, the work product of an investigation is more likely to attract privilege if a lawyer conducts the investigation and presents the findings as legal advice to their client. This is because legal advice privilege is more likely to apply to such a communication. In the context of litigation privilege, the involvement of lawyers is one element that a court will look at when applying the above test, but the involvement of lawyers is not solely determinative.

Under English law, communications with in-house lawyers will be privileged if made for the purpose of giving or obtaining legal advice rather than for general managerial or business purposes.

51 *Brownell v Roadway Package System*, 185 FRD 19 (NDNY 1999).
52 *Ibid*, 13; see also *Burlington Indus v Ellerth*, 524 US 742 (1998); *Faragher v Boca Raton*, 524 US 775 (1998).
53 *Pray v New York City Ballet Co*, 1997 WL 266980, at *1 (SDNY 1997), aff'd in part and rev'd in part, 1998 WL 558796 (SDNY 1998).
54 *Pray*, 1998 WL 558796, at *2–3.

Whether privilege applies depends on the facts and work product will not always be privileged even if a lawyer conducts the investigation.

France

Although French law does not allow communications of in-house lawyers ('*juristes*') to be covered by legal privilege under professional secrecy rules, such communications are not totally without protection. Thus, the Paris Court of Appeal ruled in the so-called *Whirlpool* case of 8 November 2017 that emails or documents that do not originate from or are not addressed to a lawyer are covered by professional secrecy 'as long as they reproduce a defence strategy put in place by [external counsel]'.[55]

In-house lawyer documents commenting on, setting out or applying the strategy defined by external counsel should therefore be covered by professional secrecy; seizure of such documents therefore infringes the rights of the defence.

Nevertheless, the question arises of the definition of what the strategy implemented by the lawyer is and to what extent the protection is effective. In addition, this precedent only relates to the seizure of documents by the French Competition Authority.

Finally, it should be noted that the decision of the Paris Court of Appeal of 8 November 2017 has been overturned by the French Court of Cassation.[56] Even if the Court of Cassation has not directly ruled on the application of professional secrecy to in-house lawyers, the judgment of the Paris Court of Appeal was entirely overturned and the case was again referred to the Court of Appeal for a new judgment to be handed down.

In conclusion and for the time being, there are no legal rules or case law in France confirming that professional secrecy applies to in-house counsel. The utmost caution must therefore be observed in this matter.

Germany

Since corporate counsels have no right to refuse testimony in criminal proceedings regarding any information received as an employee of their company, there is also no corresponding protection against seizure. This means that in general the internal communications between the management of a company and its in-house counsel with regard to an internal investigation may be seized by a public prosecutor.

However, any communications between the external criminal legal representative of the company and corporate counsel do enjoy protection against seizure if the aforementioned requirements are met. This is because communications with the external criminal legal representative of the company are protected, as aforementioned. (In Germany, these external counsels are not called 'defence attorneys' since criminal liability does not attach to corporations.)

Italy

In-house lawyers are not protected by attorneys' professional secrecy. For limited exceptions, lawyers bound by an employment relationship cannot be admitted to the Italian Bar and thus are deprived of all rights and privileges attaching to the independent legal profession.

It can be concluded that the maximum protection available from a legal privilege perspective for the information produced in the course of an investigation is ensured with reference to documents stored at the premises of a defence attorney appointed with the formalities provided by the ICCP for the defensive investigation.

55 Court of Appeal of Paris, 8 November 2017, No 14/13384.

56 Cass crim, 13 June 2019, No 17-87.364.

Malaysia

The legal position in Malaysia with regard to whether communications with in-house counsel or foreign counsel is covered by legal professional privilege is unclear. In the High Court case of *Toralf Mueller v Alcim Holding Sdn Bhd* [2015] MLJU 779, the judge in obiter interpreted Article 126 of the Evidence Act 1950 as not extending the scope of legal professional privilege to external or in-house legal counsel, and although he was in favour of the same, he viewed it as a matter for parliament.

Similarly, Article 126 of the Evidence Act specifically restricts the application of privilege to 'advocates', defined in the Interpretation Acts 1948 and 1967 to be 'person[s] entitled to practise as an advocate or as an advocate and solicitor under the law in force in any part of Malaysia'. As such, legal professional privilege in Article 126 would likely only be extended to Malaysian advocates.

Hence, it is possible that legal professional privilege under the Evidence Act extends only to practising advocates in Malaysia and not to in-house counsel or foreign counsel, although this (and the question of the application of litigation privilege, if any, to such counsel) is not a fully settled issue.

The Netherlands

If the investigation is carried out by a lawyer, privilege should attach to the investigation and its findings. Lawyers may instruct other parties (such as forensic accountants or other experts) to assist or advise in relation to an internal investigation. The prevailing view is that – if instructed by a lawyer – the activities and findings of such other parties will be covered by privilege as well. However, there is debate as to whether privilege can be claimed over work of such third parties if, in short, the role of the lawyer is merely to provide privilege over the work of third parties that are not themselves entitled to privilege. It is our view that if the lawyer's role is substantive, both in terms of the legal advice or legal representation sought by the client and in instructing and steering the third party, privilege should attach to the work and work product of the third party.

In principle, investigations carried out by in-house counsel should also be covered by legal privilege. However, privilege over those investigations – especially if the investigation is from a practical perspective carried out mostly by non-lawyers (such as an internal audit or compliance) – may be more readily challenged by public authorities.

US

In *Upjohn Co v United States*, the US Supreme Court held that a corporation's attorney–client privilege extends to investigative interviews with both management and non-management employees, so long as the investigation is undertaken at the direction of management and for the purpose of providing legal advice. To preserve the privilege, among other things, it is important during the initial investigation to take particular care in issuing Upjohn warnings to company employees. An appropriate Upjohn warning must make clear that the investigating attorney represents the company and not the interviewee, the interview is covered by the company's attorney–client privilege and that the company may elect to disclose privileged information as part of a government investigation.

For the privilege to apply, the attorney must have been acting for the purpose of obtaining legal advice. In *HSBC Guyerzeller Bank AG v Chascona NV,* Index No 114705/2003 (Sup Ct, NY County, 23 June 2010), the New York County Supreme Court held that the attorney–client privilege did not protect documents created by an attorney who was employed by creditors as 'Senior Vice President, Special Projects', during an investigation he conducted of the debtors. The court held that the attorney's work was investigative rather than legal and 'an investigative report does not become privileged merely because it was conducted by an attorney'. The Court found that the attorney served in a non-legal role, and noted that his job description made no mention of his performing legal services. The Court also dismissed as 'conclusory' the attorney's affidavit describing his work as 'predominately, if not exclusively legal'

On the other hand, in *Spectrum Services International v Chemical Bank*, 78 NY 2d 371 (1991), New York's highest court upheld as privileged a report carried out by an external law firm retained for the specific purpose of investigating possible internal fraud by employees and vendors, where affidavits of the firm's lawyers made clear that Chemical had retained them specifically to perform an investigation and render legal advice regarding this possible fraud, and to counsel Chemical with regard to possible litigation.

To what extent does legal privilege apply when dealing with public authorities?

Canada

Privilege may be enforced against governmental authorities, subject to certain exceptions. The general rule in this regard is that the power to compel disclosure of privileged information must be expressly provided under law, which law must meet certain criteria for validity.

Access to information laws, which force government entities to provide the public with access to information and documents, typically contain exceptions shielding privileged communications from disclosure.

England and Wales

A document that is protected by privilege is protected for all purposes. Therefore, investigating authorities cannot legally compel a company to produce documents that are protected by privilege.

However, investigating authorities may ask for voluntary production of privileged information, and might not view a company as fully cooperative if such a request is denied.

France

Given the absolute nature of professional secrecy, it is also conceived as a prerogative that the lawyer and their client may exercise it against public, administrative or judicial authorities. The right to professional secrecy often takes precedence over other imperatives. In principle, legal privilege can be invoked, for example, to prevent disclosure of documents to the Competition Authority.

The particularly general nature of professional secrecy reflects the legislator's desire to provide the widest possible scope of protection. However, some administrative authorities often challenge the application of legal privilege or try to reduce its scope. For example, the French financial markets authority, the AMF (*Autorité des marchés financiers*) regularly puts forward its view of legal privilege, according to which an email where a lawyer is only copied (and not one of the principal receiver) in an email from one of their clients is not confidential and can therefore be exploited.

However, if AMF investigators impose disclosure of privileged documents, this should result in annulment of the investigation procedure.

By way of exception, legal privilege cannot be invoked against some other authorities, such as the URSSAF (authority in charge of collecting social security contributions) or the DGCCRF (directorate-general for competition, consumer protection and anti-fraud investigations).

Where legal privilege is enforceable, the judge must first determine whether the documents constitute correspondence relating to the rights of the defence and, second, must cancel the seizure of documents that they find to be covered by legal privilege due to the principle of professional secrecy of relations between a lawyer and their client and the rights of the defence.

Germany

Protection against seizure according to German law, as described, naturally applies when dealing with public authorities, in particular public prosecutors.

Italy

Documents stored at the client's premises are certainly more vulnerable, since they are protected only if properly marked and to the extent they are inherent to the exercise of the client's right of defence in the criminal proceedings.

In practice, protection granted by legal privilege for documents held by the client is not very effective in the stage of pre-trial investigations conducted by public prosecutors. Enforcement of the privilege may be more effective at the trial stage, to prevent the judge from using as evidence the documents covered by legal privilege produced by the public prosecutor.

Malaysia

Article 126 of the Evidence Act 1950, which prohibits advocates from disclosing privileged information, does not specifically limit the application of privilege to the courts. The recent case of *Bar Malaysia v Ketua Pengarah Hasil Dalam Negeri* (OS No WA-24-12-03/2017, 2 April 2018) may indicate that privilege may be invoked by advocates against public authorities (the director-general of inland revenue in this case). However, Article 129 states that a person shall not be compelled to disclose 'to the courts' any privileged information. In light of the way Article 129 is drafted, the privilege in the article is likely to be restricted only to the production of evidence in court and may not be invoked when dealing with public authorities. Although the position of whether litigation privilege may be extended to dealings with public authorities is unclear, given that the policy reason underlying litigation privilege, as stated in *Wang Han Lin & Ors v HSBC Bank Malaysia Berhad* [2017] MLJU 1075, is that a party in litigation should not benefit from privileged documents prepared by their opponent, it is possible that its application may also only be restricted to production of the documents in court.

The Netherlands

In practice, legal privilege on internal investigations carried out by lawyers is observed by regulators, criminal authorities and courts. Regulators and criminal authorities remain, however, very sceptical of legal privilege and challenge privilege claims from time to time (in addition to asking clients to waive privilege). Depending on the legal context (administrative, criminal or civil law) there are various (legal) mechanisms in identifying and where necessary testing (claims of) privilege over information.

US

The privilege applies equally when dealing with public authorities as when dealing with private parties. However, even if investigative materials are privileged, a company may find it has little choice but to waive that privilege during a government investigation. In August 2008, the Department of Justice (DoJ) released its Principles of Federal Prosecution of Business Organizations, commonly referred to as the Filip Memorandum. It makes clear that the DoJ cannot compel a corporation to waive its 'core' attorney–client privilege and that a corporation need not do so to receive 'cooperation credit' under the Federal Sentencing Guidelines.

Before the implementation of the Filip Memorandum, corporations were often pressured to waive their attorney–client privilege and received more favourable treatment in exchange for doing so. Still, the Filip Memorandum also explains that, to receive cooperation credit, the corporation must disclose the 'relevant facts of which it has knowledge'.

While government pressure on companies to waive their attorney–client privilege has abated somewhat in recent years, the DoJ and the SEC continue to expect and reward disclosure of all 'relevant facts'. The Federal Sentencing Guidelines afford corporations more favourable treatment at the sentencing stage if they can demonstrate rigorous internal compliance policies and procedures. Moreover, the Department of Justice and SEC give companies cooperation credit when conducting investigations of alleged wrongdoing.

Similarly, the SEC enforcement manual indicates that it will extend cooperation credit in exchange for disclosure of 'all relevant underlying facts within [the company's] knowledge'. The distinction between privileged communication and relevant fact is a slippery one, particularly with regard to an attorney's conclusions and findings during an internal investigation. Thus, despite the government's recent efforts to limit the pressure to waive attorney–client privilege, the emphasis on full disclosure of facts gleaned during an investigation may still prompt the production of privileged information.

The doctrine of 'selective waiver' permits the privilege holder to produce privileged material to the government, while preserving privilege claims as to third-party litigants. However, the US Court of Appeals for the Second Circuit, with jurisdiction over New York, Connecticut and Vermont, has rejected the application of selective waiver where there is the existence of an adversarial relationship between the disclosing party and the government agency. However, in *In re Steinhardt*, 9 F.3d 230, 234 (2d Cir. 1993), the Court declined to adopt a per se rule against selective waiver and held that its applicability should be assessed on a case-by-case basis, recognising that it may be appropriate where the disclosing party and the governmental agency have a confidentiality agreement in place.

On the other hand, disclosure to the federal Consumer Financial Protection Bureau (CFPB), federal banking agencies, state banking supervisors or foreign banking authorities is statutorily protected from privilege waiver. The Financial Services Regulatory Relief Act 2006 amended the Federal Deposit Insurance Act, 12 USC s 1828(x), to provide that information provided to a federal banking agency, state banking supervisor or foreign banking authority 'for any purpose in the course of any supervisory or regulatory process of such agency' shall not be construed as a waiver of 'any privilege' that person may claim with respect to the information as to any third party. The section was later amended to add the CFPB. It is unclear whether this provision would be applied to bar waiver claims as to information submitted to a bank authority in the context of the authority's enforcement role, as opposed to its supervisory or regulatory role.

How does legal privilege work when conducting cross-border investigations: does it apply even if the lawyer is not in the same jurisdiction as their client?

Canada

With respect to Canadian attorneys conducting investigations outside Canada, privilege would typically still apply to the extent that the matter is governed by Canadian law. The law is not settled with respect to the applicability of privilege to foreign attorneys conducting investigations in Canada. In fact, privilege only applies to a communication between a 'solicitor' and a client, and the law is not settled on whether 'solicitor' in that context means a solicitor licensed to practise in the relevant Canadian jurisdiction, or if it goes broader than that. There are authorities on both sides of this emerging legal debate.

England and Wales

Courts and investigating authorities in England and Wales will apply English law of privilege when deciding if a document is protected by privilege.

However, under English law, the advice of foreign lawyers is protected by privilege in the same way as the advice of English lawyers.

Legal advice can be privileged under English law even if: (1) the lawyer and their client are in different jurisdictions; and (2) neither the lawyer nor their client is in England and Wales.

France

The question of whether legal privilege will apply in an internal investigation conducted by a foreign lawyer in the jurisdiction where the company is established has not been settled by French law.

The only decision to our knowledge that may be useful was issued by the Court of Cassation on 1 June 2016 (1st Civil Division, 1 June 2016, No 15-13.221):

> '… considering that the French judge, when he states that foreign laws are applicable, must understand the said laws, either thanks to the party claiming their application, or thanks to all parties, or by himself if necessary, in order to give an answer in accordance with the said foreign laws;
>
> considering that to reject the claim refusing the production of correspondence between American and Canadian attorneys, the court held that these documents were not confidential, and were therefore not covered by French professional secrecy rules;
>
> whereas the court misinterpreted the law and should instead understand the said laws to apply them to the case at hand'.

Thus, when foreign law is applicable, foreign professional secrecy rules must be applied by the French judge in accordance with the said foreign law. In other words, if an internal investigation conducted in the US is protected by professional secrecy under American law, the French judge, faced with a dispute for which American law is applicable, must then apply American law and respect foreign professional secrecy.

However, the decision does not settle the question of whether French professional secrecy can be invoked in respect of an investigation carried out in France by a lawyer of a foreign bar.

In our opinion, there is a significant risk that the lawyer of a foreign bar may not be able to invoke French professional secrecy rules. When a cross-border investigation is partly conducted outside France by a foreign lawyer, it is therefore recommended that a French lawyer be consulted or, at the very least, involved in the exchanges.

Germany

In this regard the Jones Day decisions by the Constitutional Court on June 27 2018 are also very important.[57] Not only Volkswagen AG but also the law firm Jones Day, which included three German attorneys, claimed constitutional rights.

According to the Constitutional Court, Jones Day could not base its claims on German constitutional laws as the law firm was not seen as a domestic legal entity (Article 19(3) of the German Constitution). Where the legal entity has its effective seat is the deciding factor (the so-called 'seat theory'), not the nationality of the individuals representing the legal entity. The seat follows the principal office, which is the place where the company's ultimate decision-making body takes the bulk of managerial decisions. However, the Constitutional Court did not treat Jones Day, a company founded according to the laws of Ohio/the US, as a German domestic company nor as a company with a seat in any other EU Member State. The Court also declined any exception to this rule. Jones Day could have argued that its Munich premises had to be treated like a domestic company in light of its deep involvement, its independent company structure and its Germany-centred business. Jones Day had not presented any evidence in this respect.

57 German Constitutional Court, 27 June 2018, No 2 BvR 1562/17, No 2 BvR 1287/17, No 2 BvR 1583/17.

With regard to the three German attorneys at Jones Day, the Constitutional Court argued that they had not successfully claimed that their own constitutional rights were violated by the corresponding search conducted by the public prosecutor's office in Munich.

Italy

Attorneys admitted to the Italian Bar enjoy the protection of professional secrecy irrespective of whether the client is located in Italy or abroad.

Attorneys admitted to practise in a foreign jurisdiction should enjoy the protection of professional secrecy as well, since the applicable provisions of the ICCP only make reference to 'attorneys' without any limitation as to the jurisdiction of practice. There is no precedent, however, confirming this conclusion with reference to lawyers. We found a precedent where the possibility to claim professional secrecy privilege in connection with witness statements was granted to a foreign licensed private investigator; in another case, on the other hand, the same possibility was denied to a foreign licensed accountant.

The Netherlands

From a Dutch law perspective, legal privilege of a Dutch lawyer applies irrespective of the nationality, law of incorporation, corporate seat or residence of the client. Under Dutch law, we believe that the existence and scope of legal privilege will be assessed according to the *lex fori*. In cases involving foreign lawyers, Dutch courts are therefore expected to apply Dutch legal privilege standards to determine the existence and scope of legal privilege. Although not settled in case law, if under the laws applicable to the foreign lawyers their legal privilege has a narrower scope or applicability, Dutch courts could take this into account.

Are there any data protection regulations in the jurisdiction that would make it difficult to conduct an internal investigation?

Canada

Data protection legislation in Canada does not materially have an impact on investigations. Employee consent must be obtained before disclosure of personal information by the employer to third parties; however, most privacy laws contain exceptions for third-party service providers. These exceptions allow employers to disclose personal employee information to a third-party service provider, without employee consent, if said information is to be used solely for the purpose of providing the services in question.

England and Wales

Organisations and investigators must comply with the EU General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

France

As in any other EU Member State, the GDPR is directly applicable, and has been incorporated into French law. French law No 2018-493 of 20 June 2018 amended the French data protection law (loi informatique et libertés) of 6 January 1978 to implement some of the 'flexibility' authorised by the GDPR.

France has also applied since 26 July 1968 a law known as the loi de blocage. This prohibits, without prejudice to international treaties or agreements, any natural or legal person of French nationality or habitually resident or established on French territory from communicating in writing, orally or in any other form to foreign public authorities or courts any documents or information of an economic, commercial, industrial, financial

or technical nature, should such communication be likely to prejudice French sovereignty, security, essential economic interests or public order.

Germany

The GDPR is directly applicable. In addition, compliance with the German Federal Data Protection Act (Bundesdatenschutzgesetz) is mandatory.

Italy

Pursuant to the Code of Conduct for processing personal data in the performance of defensive investigation, approved in 2008 by the Italian Privacy Authority, attorneys conducting defensive investigations must be respectful of the data subject's rights, freedom and dignity, and act in compliance with the principles of purpose limitation, necessity, proportionality and data minimisation.

Data privacy in Italy is now governed by the GDPR. It allows personal data processing, among other things, when: (1) the data subject has given consent; (2) processing is necessary for compliance with a legal obligation of the controller; or (3) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. The need to carry out a defensive investigation under the ICCP, in light of a pending criminal investigation of the public prosecutors or in anticipation of possible criminal proceedings, falls within the scope of the 'legitimate interest' provided by Article 6(f) of the GDPR, and thus the consent of the data subject is not required.

The controller of the personal data shall provide the data subject with the information regarding the data processing established by Articles 13 and 14 of the GDPR in advance. However, the information can be omitted if:

- the data subject was already informed (eg, by way of a corporate policy properly published and notified);
- if personal data will not be obtained from the data subject (eg, is stored on the corporate servers) and:
  - the provision of such information is likely to render impossible or seriously impair the achievement of the objectives of the investigation; or
  - the personal data must remain confidential subject to an obligation of professional secrecy regulated by EU or Member State law, including a statutory obligation of secrecy.

Additionally, where the outcomes of the internal investigation are to be used for purposes linked to the employment contract with the employee subjected to control (eg, for disciplinary action), the employment law restrictions on 'remote' monitoring of workers should also be duly taken into account. Specifically, according to Article 4 of Law No 300 of 20 May 1970 (the so-called Workers' Statute), which was amended in 2015:

1. installation and use of 'equipment' that allows the employer to, even only potentially, monitor or reconstruct activities performed by employees (eg, video surveillance, specific software for remote monitoring of computer activity and emails), are lawful only if:
   - they are justified by organisational, production-related or safety reasons; and
   - a prior agreement is reached with the works councils (or a prior authorisation has been given by the competent labour office);
2. the former requirements and limitations do not apply to the equipment that the worker uses to perform activities (ie, computer or email); and
3. the information collected pursuant to both the provisions described under points (1) and (2) may be

lawfully used for all purposes linked to the employment relationship (eg, disciplinary action) to the extent that the workers are adequately informed about the use of such instruments and the controls that the employer may perform through their use, by means of a corporate policy.

Before the amendment of Article 4, case law held the opinion that so-called defensive controls (ie, those addressed to ascertain illicit conduct of workers that may pose a threat to the corporate assets) were out of the scope of application of the provisions on 'remote' monitoring (ie, they could be lawfully performed even in the absence of the legal requirements imposed by Article 4 before its amendment).

Even after the amendment of Article 4, whether or not the 'defensive controls fall within the scope of application of Article 4 is still very controversial (the few case law decisions issued on the matter took different positions on this aspect).

In conclusion, under both data protection and employment principles, employers should adopt and publish a corporate policy governing the use of IT resources by the employees. Such policy should prevent or discourage employees from using corporate devices and email accounts for personal purposes, and should inform them that the communications and any other data exchanged by, or stored on, the corporate IT resources may be subject to ex-post corporate investigations for defensive purposes or to comply with a request from public authorities. Furthermore, depending on the circumstances and the kind of investigation performed, additional fulfilments (such as specific ad hoc information to the employees subjected to the investigation) may be required or advisable (thus requiring a case-by-case assessment).

Finally, in all cases of investigations on employees, the employer is not allowed to investigate the private life of employees (including, eg, political and religious opinions).

Malaysia

In Malaysia, the processing of personal data is regulated under the Personal Data Protection Act 2010 (PDPA). Under the PDPA, personal data may not be processed unless with the data subject's consent, or where the processing falls within one of the exceptions provided for within the PDPA.

The PDPA only applies to personal data in respect of commercial transactions. We take the view that the processing of personal data in internal investigations may not be considered processing in respect of commercial transactions, and as such would not fall within the scope of the PDPA. However, as the employment relationship is a commercial transaction, to ensure an unfettered ability to conduct investigations it is generally recommended that an employer ensure consent is obtained from employees for internal investigations or disciplinary proceedings in the usual course of business when obtaining the consent of employees to process their personal data for other aspects of the employment relationship.

In the alternative, the data user may seek to rely on the exceptions in the PDPA to process the personal data without consent (such as the exception for the administration of justice), but this has not yet been tested in the courts.

The Netherlands

The Netherlands is subject to the GDPR. Therefore, data protection regulations apply to internal investigations carried out by lawyers on behalf of clients. In our experience, the GDPR and local data privacy and state secrecy laws impose several formalities and principles to be observed, including to obtain and subsequently process personal information from other jurisdictions, but those can typically be navigated, although some state secrecy laws can present real obstacles.