Clifford Chance

BRIEFING

Workplace Investigations – Quarterly Review – Edition 6

June 2026

In this Quarterly Review, we spotlight the global impact of AI on workplace investigations. We examine how AI is reshaping the fact-finding process and explore the opportunities and risks of AI-assisted investigations, including recent privilege decisions, the evidential significance of AI prompts in disciplinary proceedings and the growing challenge of AI-generated evidence.

We also consider the implications for employers of AI-generated complaints and grievances and examine a recent Australian decision in which the Fair Work Commission held that an employee's excessive use of AI to generate adversarial communications during an investigation made him "ungovernable" and justified dismissal.

Beyond AI, we consider several significant legislative and case law developments that could reshape the investigations landscape.

In the UK, from October 2026, the Employment Rights Act 2025 ("ERA") will impose an enhanced duty on employers to take all reasonable steps to prevent sexual harassment and impose liability for third-party harassment (of any type) of employees at work. Employers will therefore need to plan how they investigate incidents involving third parties such as customers and suppliers. We also look ahead to the removal of the qualifying period for unfair dismissal protection and the statutory compensation cap from January 2027, which will significantly increase the stakes of dismissal decisions, particularly for senior and regulated employees.

We also consider the implications of the Crime and Policing Act 2026 in the UK, which from 29 June 2026 introduces a new statutory route to corporate criminal liability where a senior manager commits an offence within the scope of their authority – a compliance and governance development and one which may become the focus of future workplace investigations.

In France, recent case law provides further clarity over the scope of employers' obligations to conduct internal investigations and the procedural rights of employees and we consider developments in Spain, where a new Independent Whistleblower Protection Authority ("AINPI") has been established to oversee internal reporting systems.

In a financial services sector focus this Quarter we consider the impact on workplace investigations of the first wave of changes implementing the streamlining of the Senior Managers Certification Regime ("SMCR") and in particular guidance on what can be said about unfinished workplace investigations within a regulatory reference, the interaction of privilege with disclosure duties, and individual senior management responsibilities.

KEY ISSUES

1. **AI and workplace investigations (and interaction with privilege and data privacy):** Use of AI tools in investigatory scoping, AI generated grievances and evidence, and disclosure.
2. **UK Legislative changes:** Employment Rights Act 2025 and Crime and Policing Act 2026 impact the approach to investigations and governance frameworks.
3. **UK case law lessons:** The importance of a balanced investigation – *Nayfeh v Barclays Bank*.
4. **France:** No obligation to conduct an internal investigation; limits to the internal investigation process; personal data and investigations
5. **Spain:** New whistleblowing mechanism and the Independent Whistleblower Protection Authority ("AINPI").
6. **Sector focus:** UK financial services – the impact of SMCR streamlining on investigations.

EXECUTIVE SUMMARY

CROSS JURISDICTIONAL: AI and workplace investigations (Europe, APAC and US)

- The rapid adoption of AI tools by employees and employers is having a significant impact on the scope and conduct of workplace investigations. As well as assisting with streamlining the investigation process, we are seeing the use of AI to generate unwieldy grievances and possibly create evidence. Employers will need to adapt their approach to tackle these issues, including by using AI to assist with scoping grievances and training decision makers on identifying potentially employee-fabricated evidence.
- **AI & Privilege:** Recent judgments in the UK and US give insight into how the courts globally may approach privilege and AI use. In *United States v. Heppner*, a court held that materials prepared using an open source AI tool independently of legal counsel were not privileged; while in *Warner v. Gilbarco* (where the Claimant was not represented), a court refused to compel disclosure of AI-assisted litigation materials, treating AI as a functional tool to prepare litigation materials rather than a third-party disclosure; in *Munir v. Secretary of State for the*

Home Department the judge warned of the potential impact of open source AI tools on legal privilege These cases underscore that the treatment of AI privilege will turn on traditional principles such as confidentiality and the involvement of legal counsel.

EUROPE

- **UK Employment Rights Act 2025 – Third-Party Harassment:** From October 2026, employers will be subject to an enhanced duty to take *all* reasonable steps to prevent sexual harassment and will also face liability for all forms of third-party harassment of employees during employment. This is likely to increase the need for employers to investigate third-party conduct and raises complex practical questions around access to evidence and witnesses from third parties. Companies may wish to consider whether their contractual arrangements with third party providers, for example contractors and consultants, need to address this issue.
- **UK Employment Rights Act 2025 – Unfair Dismissal:** From 1 January 2027, the qualifying period for unfair dismissal protection will reduce from two years to six months, and the statutory compensation cap will be removed. These reforms will significantly increase the stakes of dismissal decisions, particularly for senior and regulated employees, and place a greater emphasis on conducting robust investigation and disciplinary processes.
- **UK Case Law – Balanced investigations:** In *Nayfeh v Barclays Bank UK Plc*, a Scottish tribunal found a dismissal unfair where the employer failed to investigate potentially exculpatory evidence with the same rigour as incriminating factors. In light of the removal of the unfair dismissal compensation cap, this is an important reminder that investigations must be balanced and wide-ranging, particularly where a dismissal outcome could have career-long consequences.
- **UK – AI, Automated Decision-Making and DSARs:** The Data (Use and Access) Act 2025 introduces a more permissive framework for automated decision-making which is relevant where AI tools are used to assist with decision making as part of an investigation. Forthcoming ICO guidelines on automated decision-making and DSARs involving AI prompts are expected in summer 2026. Employers should review and update their data protection policies and DSAR review protocols accordingly.
- **UK – Crime and Policing Act 2026:** From 29 June 2026, corporate criminal liability is introduced where a senior manager (broadly defined to include those in the direct chain of management, e.g. the CEO and the CFO, and strategic roles such as within HR) commits any offence within the scope of their authority. There is no compliance defence; robust governance, training, and whistleblowing frameworks are the primary means of mitigation.
- **UK – Interim relief in whistleblowing:** Interim relief applications in whistleblowing cases before employment tribunals have risen sharply, with AI identified by the President of the Employment Tribunal (England and Wales) as a significant factor in the increasing length and complexity of submissions. In response, new Presidential Guidance confirms that AI use is not prohibited, but litigants remain

responsible for ensuring that AI-assisted submissions are concise, relevant, accurate and focused on the key issues.

- **France – Decisions on conduct of investigations:** The Cour de Cassation has confirmed that the French Labour Code does not require an employer to conduct an internal investigation following allegations of sexual harassment; witness statements and police complaints may be sufficient to establish the facts. Separately, the Conseil d'Etat has upheld a decision by the CNIL (French Data Protection Authority) warning an employer for failing to respond adequately to data subject access requests from employees involved in an internal harassment investigation, confirming that GDPR access rights must be properly addressed during investigations while retaining the ability to redact information that would infringe the rights of others.
- **Spain – New whistleblowing authority:** A new Independent Whistleblower Protection Authority ("AINPI") has been created in Spain, with a consultative role expected to develop the whistleblowing framework through guidance and recommendations.

APAC

- **Australia – Employee AI use in investigations:** The Fair Work Commission has held that an employee's excessive use of AI to generate adversarial communications during an investigation rendered him "ungovernable" and justified dismissal, notwithstanding the employer's procedural shortcomings.

SECTOR FOCUS

UK Financial Services

SMCR Phase 1 reforms (April, July and September 2026): The FCA and PRA have introduced the first wave of SMCR streamlining changes, with further reforms taking effect in July 2026. Key changes relevant to investigations include new guidance on regulatory references where an employee departs mid-investigation and new Handbook guidance which clarifies that Senior Managers have a personal obligation to self-report certain matters, including criminal proceedings and fitness and propriety events, directly to the FCA under Conduct Rule 4, and that a failure to ensure the firm meets its own notification obligations in their area of the business may constitute a breach of Conduct Rule 2 (and that the fact that privileged communications are in train does not prevent a notification duty).

FULL REVIEW

AI and workplace investigations

Key principles

The increasingly rapid adoption of a variety of bespoke and open-source AI tools by both employees and employers is starting to have a significant impact on the scope and conduct of workplace investigations.

The demonstrable fairness and governance of investigations will matter more than ever.

In this context the use to which AI is put by employer and employee may be significant in several respects:

(1) the increasing use of AI by employees to generate lengthy grievances and claims for investigation;

(2) whether and how AI can be used to expedite and scope an investigation, review large volumes of relevant materials, and to transcribe interviews;

(3) the disclosure risks around the use of AI tools including whether, and in what circumstances, AI prompts and responses may (and may not be) be protected by privilege;

(4) the risks around AI being used by employees to fabricate evidence to support grievances and how this should be addressed; and

(5) the extent to which evidence of prompts can be leveraged as part of an investigation.

AI-generated complaints and grievances

Employers are increasingly receiving voluminous AI drafted complaints/ grievances and claims from employees. AI may, for example, insert protected disclosures or allegations of discrimination or harassment often without any factual detail or be over elaborate in the language used. AI also often includes irrelevant content and mischaracterises complaints. This makes it difficult for an employer to identify the core complaint and run an effective investigation process as a result.

It is essential that an employer understands clearly the nature of any complaint as this will inform the scope of its investigation. Where this has been made difficult by AI, early engagement with those raising allegations can be helpful. Carefully framed questions can help to elicit a summary of the complaint (or ask for confirmation that the employer's summary is accurate).

AI tools may themselves assist in this process by structuring and distilling the issues and creating an investigation framework, but it remains key that the employer validates the outputs and seeks clarification from the employee as required. In some cases, it may be appropriate to agree the framework resulting from this with the individual complainant before the investigation starts.

Local Focus: Australia

In March 2026, Australia's employment tribunal, the Fair Work Commission ("FWC"), delivered a reminder that a complainant may be held accountable for their own conduct during workplace investigations, holding that an employee's excessive, adversarial and AI-drafted communications during an investigation rendered him "ungovernable" and justified dismissal despite the employer's procedural shortcomings.

In May 2025, a bullying complaint from an employee triggered an internal investigation by FujiFilm. Throughout the investigation, the employee sent a series of lengthy, adversarial emails to HR and various managers, drafted using AI. These communications also included new allegations of sexual harassment and sex discrimination against HR. The employee also persistently attempted to relitigate a resolved incident from 2019, asserted a right to whistleblower protections and escalated his concerns to overseas FujiFilm entities, despite being advised that they were not the appropriate forum.

After finding that the complaints were unsubstantiated, FujiFilm's attention shifted to the employee's own conduct during the investigation process. Notable concerns included timesheet entries claiming 15 hours of grievance-related work in a week involving a one-hour fact-finding meeting, and false claims against a senior executive. Following a "show cause" process (a formal disciplinary step used before a dismissal decision) in respect of these concerns, FujiFilm dismissed the employee and he subsequently brought an unfair dismissal claim.

The FWC rejected the claim, criticising the employee's communications for being inappropriate and disproportionate. The FWC questioned his credibility and noted his habit of deflecting issues by making allegations against others. The FWC also remarked that his reliance on AI made his submissions dense and difficult to follow.

Ultimately, the FWC found that the employee's "*excessive*" and "*combative*" behaviour rendered him "*ungovernable*", making constructive engagement impossible. This outweighed mitigating factors, such as his long service and procedural deficiencies, including that FujiFilm had not been sufficiently direct in warning him that his conduct could lead to dismissal.

Key takeaways include:

- In Australia, the FWC is sympathetic to an employer's challenges in dealing with employees that excessively use AI to make lengthy and unreasonable, aggressive complaints;
- Employees must engage with investigation processes proportionately. A pattern of excessive and obstructive communications, particularly attempting to relitigate historical grievances or broaden complaints beyond their proper scope, may be relied upon as conduct that undermines the employment relationship;
- Assertion of whistleblower protections or external escalation in respect of workplace grievances will not preclude disciplinary action where warranted.

Employers should put an emphasis on providing clear warnings to an employee when an employee's conduct during an investigation places their employment at risk.

AI in investigatory scoping and decision-making

Once the scope of the investigation is established, AI may also support document review, chronology building and interview analysis. However, its use must be aligned with established legal principles.

In the English case of *A (appellant) v. B (respondent) [2010]* IRLR 844 the court held that an employer will not be acting reasonably if it takes an uncritical view of the information disclosed to it before contemplating taking any disciplinary action against the employee based on it. Employers must interrogate the reliability of evidence where there are grounds to do so. This principle has renewed importance in an environment where AI can generate plausible but inaccurate or incomplete output and in some circumstances may generate false evidence.

Fabricated and inaccurate evidence

There are already indications that employers are encountering fabricated evidence including screenshots of messaging exchanges produced using AI. Investigative processes will need to evolve to address this risk, including through enhanced verification steps and, where appropriate, technical analysis. Ultimately, it may not be possible to say with any accuracy whether a piece of evidence has been fabricated, so a decision maker will need to test the evidence in the usual way during interviews where possible and where appropriate reach conclusions on a balance of probabilities basis, reaching findings on plausibility.

Where AI generated transcripts and summaries are being considered as part of the evidence in an investigation, it is important to bear in mind that they should not be treated as definitive records without human review, particularly where they may later be disclosed in litigation, regulatory proceedings or DSAR responses. AI-generated transcripts and summaries can be useful, but they can also omit nuance, misattribute comments or overstate certainty. In employment disputes, that can be significant.

Leveraging AI evidence as part of an investigation

As well as being a tool that assists with running the investigation process, AI can evidence the thought process of an individual, for example, the prompts that an individual has used may demonstrate their state of mind at a particular time which could be relevant in disciplinary proceedings, e.g. if a manager denies that they witnessed a particular event, it would be useful to look at their AI prompts used during that period of time (e.g. "do I need to report [x]?"). Similarly, it may be that there is an alleged breach of AI usage policies and an individual's AI prompts need to be reviewed for that purpose.

Employers should review their retention periods for AI prompts and output (the default period may not be adequate), AI access, and ensure that privacy policies, handbooks and employment contracts are updated to advise employees of the possibility that their prompt use may be reviewed.

Privilege, disclosure and data protection issues

AI output, and the prompts to achieve it may be disclosable as part of any potential litigation, or, in response to a data subject access request ("DSAR"). In some cases, legal privilege will apply. This should be taken into account when scoping the investigation and methodology. Each case will be fact specific but relevant considerations will include:

- whether the AI tool is being used by lawyers or non-lawyers;
- whether litigation is in contemplation or not;
- whether enterprise AI is being used with protective agreements with the provider regarding data use and access, versus personal AI tools and which functionality is being used.

In the case of multi-national employers where an investigation can straddle several countries the rules on privilege and DSARs can vary and this should be factored into the investigation before any AI tools are deployed.

AI and privilege

Over the course of this year, there have been cases in both the US, UK and elsewhere addressing AI and privilege, the implications of which are being considered globally.

- *United States v. Heppner (S.D.N.Y. Feb.17, 2026)*

A criminal defendant used consumer AI to prepare defence-related materials. Significant was that the individual was represented and this decision was independent and without their counsel's direction. The New York Federal Judge held that the documents were not protected by attorney-client privilege or the work product doctrine. This is because the AI tool is not an attorney, the platform's privacy policy negated any reasonable expectation of confidentiality, and the materials were not prepared by or at the request of counsel. While it is unclear if the same decision may be reached on similar facts in other jurisdictions, there are strong arguments that a person entering a prompt into a consumer AI tool cannot have a reasonable expectation of confidentiality.

- *Warner v. Gilbarco, Inc. (E.D. Mich. Feb. 10, 2026)*

In a similar case but with distinguishing facts a self-represented plaintiff used a consumer generative AI tool, to assist in preparing litigation materials. The opposing party applied to compel disclosure of those materials, but the court refused the application. In doing so, the court emphasised that AI systems are "tools, not persons", and that sharing information with the AI tool does not amount to disclosure to an adversary, nor to disclosure in a manner likely to place the information into an adversary's hands. As a result, the requisite threshold for work product waiver under US law was not met.

Whilst these decisions are made based on the US principles of privilege, the principles that an AI tool is not an attorney and that there are limits to the ability of non-enterprise AI to attract privilege due to the lack of confidentiality may be influential in other jurisdictions.

Although there has not yet been a direct English court decision on AI and privilege, there has been early judicial commentary in the case of *Munir v Secretary of State for the Home Department* [2026] UKUT 81 (IAC). The case concerned the misuse of AI by counsel, including the reliance on hallucinated authorities. When giving its ruling, the tribunal noted:

"We also observe that to put client letters and decision letters from the Home Office into an open source AI tool, such as ChatGPT, is to place this information on the internet in the public domain, and thus to breach client confidentiality and waive legal privilege, and thus any regulated legal

professional or firm that does so would, in addition to needing to bring this to the attention of their regulator, be advised to consult with the Information Commissioner's Office. Closed source AI tools which do not place information in the public domain, such as Microsoft Copilot, are available for tasks such as summarising without these risks."

Ultimately these issues will be considered with reference to established privilege principles in the relevant jurisdiction and the decision around whether AI use is privileged will depend on the context and the type of privilege that is asserted.

- In England, where a non-lawyer, such as an employee, HR professional or executive, enters sensitive material into an enterprise AI tool and seeks what amounts to legal advice (and no litigation is underway or in reasonable contemplation), the prompt and response are unlikely to be privileged if not done at the request of their counsel: the AI is not a lawyer and there is no lawyer-client relationship. However, if the enterprise AI tool is used to prepare a draft communication to a lawyer which in turn will be for the dominant purpose of seeking legal advice, then the response (and likely the prompt too) may be privileged as inchoate communications and non-final drafts are covered by legal advice privilege.
- Confidentiality is also an important concept in determining privilege in England. In light of *Munir v Secretary of State for the Home Department*, the English courts are also likely to distinguish between enterprise and consumer AI tools. An enterprise tool deployed under contractual terms that restrict the provider's access to data preserves a stronger argument for confidentiality; a personal or consumer tool, where the provider's terms permit broad data use, is likely to negate any reasonable expectation of confidentiality.

Whether privilege applies in an investigation is a question of fact in each case, so caution should be exercised by non-lawyers in using AI, whether to seek legal advice (unlikely to be privileged) or to assist with, for example the scoping of investigations and scripts for investigation interviews (potentially privileged but very fact sensitive). The same caution should be applied with any consumer AI tools (unlikely to be privileged).

AI and Automated decision making in the EU and UK

Where AI tools are used in investigatory or disciplinary decision-making, employers should also consider the potential application of automated decision-making ("ADM") rules.

In the UK, the Data (Use and Access) Act 2025 ("DUAA") introduced a more permissive framework for solely automated decision-making, allowing it where sensitive personal data (such as health data, ethnicity or sexual orientation) is not processed and appropriate safeguards are in place. The previous UK GDPR prohibition required either meaningful human involvement or a specific exception. The Information Commissioner's Office ("ICO") has consulted on draft ADM guidelines and final guidance is expected in summer 2026. Employers using AI tools in investigative or disciplinary processes should monitor those guidelines closely.

For employers operating in the EU, any use of AI tools in an investigation or disciplinary process will need to be assessed against the applicable framework, including the EU AI Act.

The EU AI Act provisions on high-risk AI systems have been delayed until 2 December 2027. However, the European Commission's draft Guidelines on the Classification of High-Risk AI Systems indicate that the concept will be applied expansively in the employment context: AI tools used to monitor or evaluate employee performance or behaviour are likely to be classified as high-risk, with significant compliance obligations. Employers should review whether any AI tools used in investigations or to prompt an investigation fall within that classification.

In the UK, DSARs relating to investigations are increasingly including requests for AI prompts, AI-generated transcripts and meeting summaries containing personal data. Employers should review DSAR response protocols and update data protection policies to address how AI-generated material is handled. Also of potential relevance are new ICO guidelines on handling subject access requests generated by AI, that are expected in summer 2026 (For wider considerations around AI note-taking tools, see our article: *Generative AI tools in the boardroom?*)

AI and Investigations: "practical Takeaways":

- Treat AI use as part of the evidence environment, not a side issue;
- Treat documentary evidence as inherently requiring verification;
- Document human oversight of any AI-assisted analysis;
- Define investigation scope early and agree it where possible;
- Consider privilege and disclosure consequences before using AI tools;
- Ensure DSAR and investigation policies and practices support a review of AI prompts;
- Establish an evidence verification protocol for key materials including screen shots and messaging records to address the growing risk of AI fabricated evidence; consider whether technical or forensic analysis may be required if fabrication is suspected;
- Train investigators and HR teams on AI-related credibility issues; and
- In cross border investigations map the applicable data protection requirements and privilege rules before deploying AI tools as these may vary materially across the relevant jurisdictions.

UK

UK Employment Rights Act 2025 ("ERA"): Third-Party Harassment

In October 2026, the ERA will impose on employers an enhanced statutory duty to take *all* reasonable steps to prevent sexual harassment in the workplace (as opposed to the existing duty to take reasonable steps). Where that duty is breached, employment tribunals will have the power to apply an uplift of up to 25% to any compensation awarded in successful claims.

At the same time, the ERA will impose employer liability for third-party harassment of its employees in the course of employment. This will apply to all forms of harassment (not just sexual harassment) prohibited by the Equality Act 2010, unless the employer can demonstrate that it took all reasonable steps to prevent such conduct.

As a result of this legislative change employers are likely to find themselves increasingly having to investigate third-party harassment. This adds an additional layer of complexity to running an investigation. Is it possible to interview employees of third parties, e.g. customers or suppliers, or gain access to evidence that belongs to those providers? Whilst seeking to do so may create issues from a relationship perspective, failure to take steps to attempt to investigate the issue may impact the ability to use the "failure to take all reasonable steps" defence.

Employers should review contracts with consultants, agencies, suppliers and customers to ensure they have the contractual ability to require assistance with an investigation into third-party harassment. They should also ensure that suppliers and customers are required to have in place robust anti-harassment policies, or, where appropriate, to adhere to the employer's own policy (for example, in the case of a consultant or agency worker working on site).

As a preemptive step employers should conduct a risk assessment to map potentially high-risk third-party interactions and put in place measures such as reporting channels and manager escalation guidance, in addition to customer or supplier communications and contractual protections where appropriate.

Employment Rights Act 2025: Extension of Unfair Dismissal Rights

Separately, from 1 January 2027, the qualifying period for unfair dismissal protection is due to be reduced from two years to six months, and the statutory cap on unfair dismissal compensation (currently £123,543) will be removed. This reform has potentially significant implications for senior, highly paid and regulated employees, particularly where dismissal may have career-limiting consequences (for example, dismissal for non-financial misconduct in the financial services sector). As a result, we expect that there will be increased emphasis on the need to conduct a robust investigation and disciplinary process to avoid expensive litigation and settlement payments.

UK Case Law Update: The importance of a balanced investigation

The importance of a balanced investigation is illustrated by a more recent Scottish case, *Nayfeh v Barclays Bank UK Plc (Scotland)*. In that case, the tribunal found a dismissal unfair where the employer had failed to investigate potentially exculpatory evidence with the same rigour as factors pointing towards the employee's guilt. The employee was engaged in the financial services sector and was the subject of an allegation of sexual harassment; this was a classic he said/she said case. Dismissal in such circumstances, as the tribunal acknowledged, could lead to career long loss in the financial services sector.

The tribunal acknowledged that exploring exculpatory factors might lead to the uncomfortable need to explore and test the cogency of the evidence of a person who said that she had been made uncomfortable by comments of a sexual nature but that was what the situation required. In this case the tribunal was of the view that as the employer was a large and sophisticated company with considerable resources it was equipped to carry out a process with the necessary care.

This case emphasises the need for an investigation to be balanced and wide ranging to avoid it being challenged as being procedurally unfair.

The removal of the unfair dismissal cap brings the risk of failing to do so into sharp focus, particularly in situations where a disciplinary investigation outcome could lead to the individual being unable to work in their professional sector again, leading to career long losses that could be recoverable against the employer.

The Crime and Policing Act 2026

From 29 June 2026, section 250 of the Crime and Policing Act 2026 ("CPA") is in force. This provides that where a senior manager of a body corporate or partnership commits any criminal offence while acting within the actual or apparent scope of their authority, the organisation also commits the offence; providing a new statutory route to corporate liability for all offences. The definition of senior manager covers both those in the direct chain of management (e.g., CFO, COO) as well as those in strategic roles, irrespective of their title, remuneration, qualifications, or employment status; for example, HR.

There is no compliance-defence available. However, effective mitigation is likely to include identifying and investigating situations in which individual conduct could expose the organisation to liability (and in light of any findings revisiting governance and senior-manager control). This should be supported by robust training, policies, contractual provisions and other compliance culture measures (including effective whistleblowing policies, delegation/ escalation approaches and management information flows to ensure visibility).

New Employment Tribunal Presidential guidance on the use of AI in interim relief applications

The volume of interim relief applications in whistleblowing cases before employment tribunals has risen sharply with parties increasingly submitting lengthy and complex documentation. The President of the Employment Tribunal (England and Wales) has identified AI as a significant driver of this trend and has issued Presidential Guidance on Interim Relief Applications in response. The Guidance does not prohibit the use of AI but places the responsibility for quality firmly on litigants; "there is no objection in principle to the use of AI, it often results in submissions that are too long and complex, contain irrelevant material and fail to focus on the key points in the case. Litigants who use AI to assist them have a responsibility to ensure that what is submitted is concise, relevant and accurate."

FRANCE

In France there have been some recent case law decisions which give direction on the investigation approach required.

The employer is not required to conduct an internal investigation following a report of sexual harassment.

- The employee, dismissed for gross misconduct on account of acts of sexual harassment, argued that the employer's failure to conduct an internal investigation demonstrated a lack of evidence supporting the allegations against him.

- Before the courts, the employer produced statements from the victims, a police complaint and witness attestations from employees who had heard the victims' accounts. These elements indicated that the accused employee had repeatedly held and attempted to kiss one of the victims against her will in the company's mailroom, and also that he has exposed himself and forced her to touch him.
- The Court of Appeal agreed with the dismissed employee, holding that the employer could not rely solely on employee statements without carrying out an internal investigation to corroborate them, and that, in the absence of such an investigation, the materiality of the alleged facts was insufficiently established.
- However, the Cour de cassation/ Supreme Court overturned this decision and clarified that no provision of the French Labour Code requires an employer to conduct an internal investigation in the event of allegations of sexual harassment. The appellate decision was therefore overturned, as the lower court's reasoning was not sufficient to disregard the evidentiary value of the statements and witness attestations produced by the employer.

Reference: French Civil Supreme Court "Cour de cassation", decision of the Social Chamber dated 14 January 2026, No. 24-19.544.

Employer discretion in running an internal investigation

- Following an internal investigation into managerial conduct which was deemed inappropriate, an employee was dismissed for gross misconduct.
- The employee challenged the dismissal, alleging a lack of adversarial process in the conduct of the investigation, in particular on the grounds that he had neither been interviewed nor "confronted with his colleagues" during the investigation, and had not been granted access to the case file or to the evidence collected by the employer.
- After his claims had been dismissed on appeal, the *Cour de Cassation* upheld the rejection of the dismissed employee's claims.
- In this case, the *Cour de Cassation* draws a clear distinction between two stages in the fact-finding process and held that the investigation phase falls within the employer's managerial authority.
- The employer is free to determine the methods and procedures of the investigation. In particular, it may collect statements it considers useful and interview the employees concerned, without being required to interview the accused employee, organise confrontations or grant access to the investigation file.
- The litigation phase follows the investigation and takes place before the courts, where the employee may challenge the evidence relied upon.
- Accordingly, procedural safeguards fully apply only at the judicial stage and not during the internal investigation.

Reference: Cour de cassation, decision of the Social Chamber dated 14 January 2026, No. 24-13.234.

Personal data and Investigations

- Three employees involved in an internal investigation, initiated following reports of harassment or discrimination, applied to the CNIL in order to exercise their rights under the GDPR. These employees objected to their employer processing their personal data in the context of the investigation and requested access to such data.
- Following the employer's failure to respond, the employees brought the matter before the CNIL, which issued a warning to the employer on the basis of several breaches: failure to state reasons for rejecting the objection, lack of clear information regarding the data processing, and failure to respond to access requests.
- The employer argued that the processing was based on a legal obligation excluding the right to object, and that the employees' access requests were manifestly excessive. The *Conseil d'Etat* (French Administrative Supreme Court) partially rejected the employer's arguments, holding, on the one hand, that the processing was not based on a legal obligation but was necessary for the purposes of the legitimate interests pursued by the data controller, and, on the other hand, that the employees' access requests was not manifestly excessive. Consequently, the employer was required to comply with the employees' access requests, while retaining the right to redact any information likely to infringe the rights and freedoms of others.
- The CNIL's decision was therefore upheld by the *Conseil d'Etat*.

Reference: French Administrative Supreme Court "Conseil d'Etat", decision dated 1 December 2025, No. 498023.

SPAIN

Recent developments have brought welcome clarity to Spain's whistleblowing regime:

- **New regulatory authority:** The Independent Whistleblower Protection Authority (AINPI) has been established. It will develop the framework through soft law – circulars, recommendations and interpretative guidance – rather than detailed statutory rules, and will receive notifications of internal reporting system manager appointments and oversee those systems.
- **Data protection clarification:** The Spanish Data Protection Agency has confirmed that the company (not the board of directors) is the data controller of the whistleblowing system, resolving a significant ambiguity and aligning the regime with GDPR principles while preserving the board's oversight role.
- **Jurisdictional consistency:** To address regional fragmentation, the AINPI has recommended that entities submit information to the state authority during this initial phase to ensure a baseline level of consistency across jurisdictions.

SECTOR FOCUS: FINANCIAL SERVICES

The first wave of SMCR phase 1 reforms came into force on 24 April 2026 (FCA PS26/6; PRA PS12/26), with further Phase 1 changes following on 10 July and 1 September 2026. Framed as a streamlining exercise rather than a fundamental overhaul, the changes most relevant to workplace investigators include:

- **Regulatory references:** Of significance is the new guidance which deals with how to address mid-investigation departures within a regulatory reference. Firms are not automatically prevented from referring to suspected misconduct if the employee leaves the business before the investigation is concluded but must have taken sufficient steps to verify the facts before doing so. The guidance requires firms to weigh up other factors before including suspected misconduct – specifically, the seriousness of the alleged misconduct, the basis for the firm's belief, its obligations to act fairly under the SYSC Handbook, and other relevant legal considerations such as privacy and employment law.
- In addition, firms receiving requests for mandatory regulatory references for Senior Manager Functions ("SMF") and certification candidates must now respond within four weeks, down from six, as part of a broader push to accelerate the onboarding process.
- **Conduct Rule notifications:** Where a firm relies on the 12-week rule to allow an unapproved individual to cover an SMF role, the Senior Manager Conduct Rules now apply to that individual during the temporary period of replacement. Any breach that results in disciplinary action must be reported to the FCA as soon as practicable – in line with the treatment of approved SMFs – rather than being swept up into the firm's annual Conduct Rule return.
- **Senior Manager accountability:** Senior Manager Conduct Rule 4 – requiring Senior Managers to disclose information of which the FCA would reasonably expect notice. The new Handbook guidance makes explicit that this is not limited to matters relating to the firm. Senior Managers must also self-report certain personal matters including criminal prosecution or conviction for fraud or dishonesty and other events that go to their fitness and propriety. Notably, this obligation applies even if the matter is, in parallel, the subject of or referred to or described in legally privileged communications, documents or other records created within or for the firm. Similarly, updated guidance on Conduct Rule 2 makes clear that a Senior Manager who fails to take reasonable steps to ensure that notifiable matters arising in their business area are escalated and reported to the FCA under Principle 11 and SUP 15 may themselves be in breach – again, legal privilege is no excuse.

Looking ahead, HM Treasury has confirmed its intention to legislate, subject to parliamentary time, to remove the Certification Regime from statute, remove the requirement for prior approval for certain SMF roles, and repeal the prescriptive legislative requirements around Conduct Rule training and breach notification. Phase 2 consultations from the FCA and PRA are expected before year-end. Firms should keep a close watching brief on the SMCR phase 2 changes. These are likely to be substantive and

have the potential to reshape misconduct investigations, the treatment of misconduct findings and notification obligations well beyond the scope of the Phase 1 reforms.

Our people are happy to discuss any of these developments. Our workplace investigations and culture hub can be found here.

For an overview of employment law in a large range of key jurisdictions see our easy-to-use digital guide:
Clifford Chance Employment Law Guide App
Access the web version or download from the App store / Google play.

Alistair Woodland
Head of UK Employment and Co-head of Global Employment, London

Email: alistair.woodland@cliffordchance.com
Mobile: +44 207006 8936

Floris van de Bult
Co-head of Global Employment, Amsterdam

Email: floris.vandebult@cliffordchance.com
Mobile: +31 20 711 9158

Chinwe Odimba - Chapman
Office Managing Partner for London / Co-Regional Managing Partner for One Europe, London

Email: chinwe.odimba-chapman@cliffordchance.com
Mobile: +44 207006 2406

Alastair Windass
Partner, London

Email: alastair.windass@cliffordchance.com
Mobile: +44 207006 2458

Amy Bird
Partner, London

Email: amy.bird@cliffordchance.com
Mobile: +44 207006 1830

Oliver Pegden
Partner, London

Email: oliver.pegden @cliffordchance.com
Mobile: +44 7535414174

Megan Catli
Senior Associate, London

Email: megan.catli @cliffordchance.com
Mobile: +44 7974853958

Clancy King
Partner, Sydney

Email: clancy.king @cliffordchance.com
Mobile: +61299478346

Dr. Ines Keitel
Partner, Frankfurt

Email: ines.keitel @cliffordchance.com
Mobile: +49 69 7199 1250

Janice Goh
Partner, Cavenagh Law, Singapore

Email: janice.goh @cliffordchance.com
Mobile: +65 6661 2021

Luke Tolaini
Partner, London

Email: luke.tolaini @cliffordchance.com
Mobile: +44 207006 4666

Simonetta Candela
Partner, Milan

Email: simonetta.candela @cliffordchance.com
Mobile: +39 02 8063 4245

Authors

Laura Conway
Senior Associate, London

Email: laura.conway @cliffordchance.com
Mobile: +44 (0)20 7006 1380

Tania Stevenson
Knowledge Director, London

Email: tania.stevenson @cliffordchance.com
Mobile: +44 (0)20 7006 8938

Maria Toma
Senior Associate, London

Email: maria.toma @cliffordchance.com
Mobile: +44 (0)20 7006 3876

Jorge Martín-Fernández
Counsel, Madrid

Email: jorge.martin-fernandez@cliffordchance.com
Mobile: +34 91 590 4101

Sophie Brill
Associate, New York

Email: sophie.brill@cliffordchance.com
Mobile: +1 212 878 3169