Privilege Pitfalls in Cross-Border MEA Investigations: Building Protection into the Process

ALERT | July 29, 2026

I. Introduction

In the **first article in this series**, we discussed some of the key decisions that arise at the outset of an internal investigation in the Middle East and Africa. One of those decisions deserves particular attention: how to preserve privilege and related legal protections once the investigation begins.

This is often easier said than done. Cross-border investigations in the region may involve conduct in one country, employees in another, documents hosted elsewhere, and legal or compliance teams coordinating from outside the jurisdiction. They may also involve a mix of common-law, civil-law, and local regulatory systems, each of which may treat privilege, professional secrecy, and disclosure obligations differently.

The result is that legal and compliance teams should not assume that privilege will automatically apply simply because lawyers are involved. In many cases, privilege protection needs to be built into the investigation from the outset, with careful attention to where the relevant conduct occurred, where documents and witnesses are located, where legal advice is being provided, and where future litigation or enforcement activity may arise.

In this installment, we explore six common privilege pitfalls to consider in cross-border MEA investigations.

II. Assuming Privilege Travels Across Borders

A common mistake is to assume that privilege can be assessed by reference to a single jurisdiction. In cross-border MEA investigations, privilege determinations typically need to consider applicable law and practice for several legal systems, including where the conduct occurred, where documents and witnesses are located, where the parent company or relevant decision-makers are based, and where regulators, prosecutors, or courts may later seek access to the investigation materials.

In some jurisdictions, communications with external counsel may receive stronger protection than communications with in-house counsel. In others, the relevant protection may be framed more as professional secrecy than litigation or legal advice privilege. Some jurisdictions may have limited guidance on whether interview notes, forensic reports, or internal investigation memoranda are protected at all. In other jurisdictions, attorney-client privilege may be limited, framed differently, or not recognized in a way that aligns with expectations.

This matters because MEA investigations often require coordination across several jurisdictions. Documents may be collected locally, reviewed by regional or global counsel, and then summarized for decision-makers elsewhere. If the privilege analysis is only considered from the perspective of one jurisdiction, the company may miss risks that arise where the documents, witnesses, regulators, or potential proceedings are located.

At the outset of a significant investigation, teams should identify the key jurisdictions likely to be involved and consider whether local counsel input is needed on privilege, document production, employment, data protection, and regulator access issues for each of those jurisdictions.

III. Failing to Define the Investigation from the Outset

Privilege issues are much harder to fix after the fact. By the time someone asks whether a memorandum, interview note, email update, or forensic report is privileged, the key decisions may already have been made.

Three questions are particularly important. First, what is the purpose of the investigation? A privilege claim is likely to be strongest where the investigation is being conducted to enable the company to obtain legal advice or prepare for potential legal proceedings. It may be weaker where the exercise is framed primarily as audit support, business remediation, HR review, or ordinary-course compliance monitoring.

Second, who will lead or direct the investigation? If legal advice is one of the purposes of the review, the role of in-house counsel, external counsel, and non-legal stakeholders should be clear. The fact that lawyers are copied on emails or attend meetings will typically not be enough if the investigation is, in substance, being conducted for a non-legal purpose.

Third, how will the findings be reported? Investigation teams should consider from the outset whether findings will be delivered orally or in writing, who will receive them, whether a report will need to be made to a third party, the public or a governmental agency, and how updates to business stakeholders will be framed.

Where the investigation is being conducted to enable the company to obtain legal advice, that purpose should be clear from the beginning. Engagement letters, investigation plans, document requests, and reporting lines should all be consistent with that purpose and documented accordingly.

This does not mean every investigation needs to be run as a full-scale outside counsel-led review. The approach should be proportionate to the risk. But where potential criminal, regulatory, sanctions, anti-corruption, or litigation exposure is involved, companies should be deliberate about who leads the investigation and how counsel’s role is documented.

IV. Circulating Investigation Updates Too Widely

Privilege risk increases as the circle of recipients expands.

Internal investigations often involve many stakeholders, including legal, compliance, HR, audit, finance, IT, local management, regional leadership, external counsel, and forensic providers. Many of those stakeholders have legitimate roles to play, but not everyone needs to receive every privileged communication, witness summary, draft report, or legal analysis.

Broad circulation can make it harder to show that communications were confidential and made for the purpose of legal advice. It also increases the practical risk that sensitive materials will be forwarded, downloaded, translated, summarized, or discussed outside the intended privileged group, thereby increasing the risk of potential privilege waiver.

Companies should consider defining a core investigation team at the outset. More general business updates can still be provided where needed, but those updates should be carefully framed and should avoid unnecessary legal analysis, or counsel's mental impressions.

This is particularly important in multilingual investigations, where privileged material may be translated or paraphrased for local teams. Where necessary, translations of underlying privileged materials should be prepared as part of the privileged workstream. This avoids the risk of team members using third-party commercial tools to translate or summarize legal analysis prepared in another language. Using such tools can expose the analysis to potential claims of privilege waiver, undermine confidentiality and distort the intended meaning of the privileged guidance.

V. Mishandling Interviews

Witness interviews can create privilege issues if they are not planned carefully.

In U.S.-style investigations, lawyers often provide a so-called "*Upjohn* warning" or similar explanation to the employee being interviewed, reminding the employee to keep the discussion confidential, and explaining that counsel represents the company, not the individual employee, and that the company controls whether to maintain or waive privilege. In MEA investigations, that concept may need to be adapted to local law and local expectations. Employees may be unfamiliar with the concept, and local employment or labor rules may affect how interviews should be conducted.

For example, local law or practice may affect whether a witness should receive written notice in advance, whether the witness may request accompaniment, whether the interview should be conducted in a particular language, how confidentiality instructions should be framed, and whether in-house counsel or HR should participate. Those adjustments should not dilute the core message that company counsel represents the company, but they may affect how that message is delivered and whether privilege will attach to the interview.

Such determinations should be made from the perspective of both the local jurisdiction and any anticipated expectations of foreign government regulators that may become involved in the future.

VI. Using Third-Party Providers and AI Tools Without Privilege Controls

Similar care is needed in engagements with forensic accountants, e-discovery vendors, translators, cyber specialists, and other consultants. These providers are often essential to the investigation, but their engagement should be structured carefully to preserve privilege and work product protections. In appropriate cases, counsel should retain and direct the provider so that the work supports counsel's provision of legal advice. It is helpful to formalize this reasoning in the engagement letters for the providers.

The same point applies to deliverables. A forensic report prepared primarily for audit, business, or remediation purposes may be treated differently from work directed by counsel for legal advice. The purpose, recipients, and handling of any report should be considered before the work begins and then documented when the report or deliverable is transmitted.

Investigation teams should also consider whether employees, legal teams, or other stakeholders may use AI tools in ways that create privilege or confidentiality risks.

In practice, AI tools may be used to summarize documents, translate materials, prepare chronologies, draft interview outlines, analyze communications, or refine investigation updates. Those uses may be efficient, but they can create risk if privileged or confidential investigation materials are entered into tools that have not been approved for that purpose.

The concern is not only whether AI-generated content is accurate. It is also whether the use of the tool could result in privileged material being disclosed outside the intended investigation team, retained by a third-party provider, used for model training, or handled in a way that is inconsistent with the company's confidentiality, data protection, or information-security obligations.

Companies should therefore be clear at the outset about whether AI tools may be used in the investigation, which tools are approved, what types of materials may not be uploaded, and when legal approval is required. As with translation and forensic support, the key is to avoid informal or uncontrolled use of tools that could undermine the privilege protections the investigation team is trying to preserve.

We will address AI in greater detail later in this series, including the practical steps companies can take to manage privilege, confidentiality, data protection, and governance risks when AI tools are used in internal investigations.

VII. Sharing Findings Without Thinking Through Waiver Risk

At some point, the company may need to decide whether to share investigation findings with regulators, auditors, insurers, lenders, contractual counterparties, or other third parties.

There may be good reasons to do so. A disclosure may be legally required. The company may be seeking cooperation credit from an enforcement authority. It may need to respond to a regulator, satisfy an auditor, or explain remedial steps to a stakeholder.

But external sharing should be planned carefully. The company should understand what must be disclosed, what it may choose to disclose voluntarily, and whether disclosure could waive privilege or create follow-on risks in other jurisdictions.

In some situations, it may be possible to provide factual information without sharing privileged analysis. In others, an oral briefing may be preferable to a written report. Confidentiality or non-waiver arrangements may also be relevant, although they will not necessarily resolve the issue in every jurisdiction.

The key point is that disclosure strategy and privilege strategy should be aligned. Once sensitive material is shared externally, it may be difficult to control how it is used, requested, or characterized by other authorities or litigants.

VIII. Key Takeaways

Privilege in cross-border MEA investigations is not just a legal doctrine. It is an investigation management issue.

Companies can reduce risk by:

- identifying privilege issues at the outset;
- defining the purpose of the investigation, who will lead it, and how findings will be reported;
- documenting key privilege, reporting, and disclosure decisions throughout the investigation;
- keeping the investigation team appropriately tight;
- separating legal advice from ordinary business updates;
- controlling the use of translation and AI tools with privileged materials;
- adapting witness warnings to local context;
- structuring forensic and consultant engagements carefully; and
- aligning disclosure strategy with privilege strategy before sharing findings externally.

The broader lesson is simple: privilege should not be treated as a label added to documents after they are created. In cross-border MEA investigations, it should be built into the way the investigation is structured, conducted, documented, and reported from the beginning through the end.

IX. Looking Ahead

In the next installment in this series, we will turn from how an investigation is structured to one of the most common triggers for investigations in MEA markets: third-party misconduct. In particular, we will consider the challenges of investigating distributors, agents, intermediaries, and other business partners in markets where third-party relationships are often essential to commercial operations but can also create significant compliance risk.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our White-Collar Defense and Investigations practice:

Ben Haley	+971 4 247 2116	**bhaley@cov.com**
Noam Kutler	+1 202 662 5587	**nkutler@cov.com**
Ahmed Mokdad	+27 11 944 6915	**amokdad@cov.com**