Knock, Knock

When Authorities Come Knocking: Do's and Don'ts During Investigations

22 July 2025

Few corporate nightmares begin as subtly as an external investigation — a knock on the door, a ring of the bell — and within seconds, everything changes. Unannounced inspections are aimed at probing legal infringements. They are highly disruptive and expose companies to serious legal and reputational risks. While most companies are aware of the risk of dawn raids by competition authorities such as the European Commission (**Commission**) or the German Federal Cartel Office (**FCO**), they should also be prepared for inspections by other agencies, such as tax and customs authorities, OLAF (**European Anti-Fraud Office**) or public prosecutors. Each authority operates under its own distinct legal framework and pursues a specific enforcement agenda, ranging from antitrust violations and breaches of customs, tax, or export control laws to criminal offences such as fraud or corruption. What all these investigations have in common: They typically come without a warning and demand an immediate, coordinated and legally sound response. This briefing provides a practical overview of what (not) to do during inspections – offering both general best practices and authority-specific guidelines.

Do's and Don'ts when navigating external investigations

Ideally, companies prepare for raids in advance and maintain a bespoke checklist on what (not) to do and which emergency contacts to inform immediately. These documents should ideally be tailored to investigations by different authorities. However, regardless of the investigating authority, certain fundamental principles and immediate actions apply universally to ensure compliance and protect the company's legal interests:

First things first: What's happening?

Clarify the situation. Request the following information from the investigators:

- **Identify the responsible authority:** Ask which specific authority has ordered the investigation.
- **Request identification and documentation:** Ask the officers to present their identification and the warrant authorising the search. Make and retain a copy of both. Note the name, position, and contact information of the officer leading the operation.
- **Review the scope of the warrant:** Carefully examine the warrant to determine whether the search is limited to specific projects, documents, or time periods.

Note down any other potentially relevant information mentioned by the officials regarding the scope.

Making the right call(s)

- **Notify legal counsel without delay:** Immediately inform both your internal and external legal counsel. Provide them with all information gathered so far. Politely request that the officials wait until your legal counsel arrives before proceeding further.

- **Appoint a company coordinator:** Designate a coordinator at the very outset of the investigation. Strictly adhere to internal reporting lines and instructions thereafter. Immediately inform your direct superiors as well as the executive board or managing directors. Ensure that the legal team and/or external legal advisors are looped into all communications with the investigators – even on technical details.

- **Avoid external communications:** Do not contact competitors or other suspected parties, as this may qualify as obstruction and trigger heavy fines. Refrain from public statements until a public communication strategy has been formed after the raid.

Monitoring the investigation

- **Comply with the scope of the warrant:** Grant the officials access to the rooms, files, or data explicitly specified in the warrant. However, there is no need to proactively guide them to evidence. If possible, provide the investigators with a conference room to use as a "base" to minimise disruptions to your business.

- **Golden Rule:** Hands off the evidence! Under no circumstances may documents, emails, files, or physical evidence be deleted, destroyed, or modified. Any breach can expose the company to massive penalties and irreparable harm. Every employee must understand that compliance with this rule is paramount.

- **Assign "shadows" to monitor the search:** If possible, allocate one "shadow" to monitor each official conducting the search. Ideally, legal counsel should act as shadows. If legal counsel is not available, trained employees may act as shadows. Ensure that no official searches or confiscates materials unsupervised.

- **Object to searches outside the scope:** Should officials actively request access to materials outside the scope of the investigation as defined in the warrant, object explicitly. Should the investigators accidentally stumble upon out of scope evidence, this can be usable. As specifics vary depending on the authority and circumstances, alert your legal counsel and discuss formally recording an objection with the authority.

- **Diligently document all search activities:** Keep detailed records of all areas searched and items seized. If laptops or computers are accessed, note precisely which search terms the officials use.

- **Do not discuss the allegations:** Do not discuss the subject of the investigation with officials. If authorities wish to question employees, ensure that legal counsel is present for any interviews.

Concluding the investigation and preparing next steps

- **Ask about planned public communications:** Towards the end of the investigation, ask the officers whether (and when) a press release is planned and whether the company will be named. Press releases are common in competition dawn raids and integrating them into your company's public communication planning is crucial.

- **Request an official record of all seized materials:** Ask for a complete and signed list of all documents, files, and objects seized during the search.

- **Initiate an internal investigation immediately:** Conduct an independent and thorough internal review of the allegations. This allows you to assess risks, control the narrative, and, if necessary, pursue voluntary self-disclosure or close cooperation to mitigate potential penalties. AI may be a helpful booster for this step (see our briefing on this here).

Investigations by the FCO and the European Commission

Investigations by the FCO or the Commission typically occur when there is suspicion of a serious breach of competition law, such as cartel infringements (e.g. price fixing schemes, market allocation arrangements, illegal information exchange), or an abuse of dominance. Immediate legal advice is particularly crucial here, as early strategic decisions — particularly **securing a cooperation marker** or placing a leniency application — can significantly influence the outcome and the amount of the fine at the end of the investigation. With a marker, companies involved in a cartel infringement can secure their position in the leniency queue, where timing is critical: full immunity or major fine reductions typically go only to the first applicant.

Although both the Commission and the FCO act as competition watchdogs, there are a few procedural differences depending on which authority is investigating. For example, the Commission may not review legally privileged **communications with external legal counsel**, whereas under German law, the concept of legal privilege is much narrower, so the FCO can generally examine such correspondence. Moreover, the Commission cannot seize documents, computers or hardware but is limited to inspection on site, while the FCO regularly exercises such powers.

The aforementioned **"golden rule" not to tamper with evidence** has caused the Commission to impose particularly **noteworthy fines**: E.ON still holds the record with €38 million for infamously breaching a seal during a dawn raid, after Commission officials had sealed a room to secure evidence overnight (and reportedly, cleaning staff broke the seal). In 2024, the Commission fined International Flavors & Fragrances €15.9 million after a senior employee deleted WhatsApp messages with a competitor during a dawn raid – a painfully high sum considering it already includes a 50% cooperation discount and that the company had explicitly instructed not to delete any data (i.e. fines don't require intent or even negligence!). Finally, the Commission has repeatedly stressed that "deleted doesn't mean gone"; its forensic teams are more than capable of recovering "lost" data. For overall guidance and quick reference on how to prepare for and behave during dawn raids, BLOMSTEIN has published emergency checklists for both FCO and Commission inspections on its website.

Investigations by customs authorities

Investigations by customs authorities in Germany may concern a broad range of suspected offences, including violations of export control regulations, breaches of customs or embargo restrictions. While the **Federal Office for Economic Affairs and Export Control (BAFA)** is formally the competent authority for licensing matters under the **Foreign Trade and Payments Act**, enforcement in practice is regularly led by the **Customs Investigation Office (Zollfahndungsamt)** in cooperation with the public prosecutor.

Such investigations are typically conducted under the **German Code of Criminal Procedure**, rather than administrative law, granting investigators significantly broader powers. These may even include covert surveillance, telecommunications interception, and undercover operations—each subject to prior judicial authorisation. Further, companies can become targets not only as suspects but also as third parties in possession of potentially relevant material. Of course, in such cases, stricter standards of proportionality and judicial oversight apply.

The (relatively) new kid on the block: Investigations by OLAF

BLOMSTEIN has already published extensive guidance on investigations by OLAF (European Anti-Fraud Office), which has only been around for a few years. The following summary only recaps the key points (for further details, see our Overview, Checklist for Investigations, Process Overview and Overview of legal remedies):

OLAF has broad powers to conduct on-site investigations and interviews, but notably, it **does not have coercive powers** and must rely on voluntary cooperation or national enforcement measures. One may also evaluate whether to challenge procedural measures or **contest findings in OLAF's final report** before the competent courts. Early legal advice is highly recommended to safeguard your rights and to mitigate reputational risks.

"Work from home" means raid at home

One current "trend" to be aware of is that the increasing popularity of remote working and home-office policies also increase raids directed at private residences. The authorities are aware that their power to raid private homes is particularly invasive and appear to handle it with care across the board. Still, companies may want to prepare senior management or colleagues working in particularly sensitive areas for this risk and give them guidance on how to react. Generally, the critical Do's and Don'ts remain sensible here.

***

BLOMSTEIN provides comprehensive support – before, during, and after a raid. Our nationwide network of experienced colleagues, the BLOMSTEIN Dawn Raid Taskforce, can be on-site at your premises within the shortest possible time to provide immediate assistance. If you have any questions, please do not hesitate to contact Anna Blume Huttenlauch, Laura Louca, Philipp Trube or any member of the BLOMSTEIN team.

BLOMSTEIN | We provide legal support to our international client base on competition, international trade, public procurement, state aid and ESG in Germany, Europe, and – through our global network – worldwide.