



Schlun & Elseven
Rechtsanwälte

Dawn Raid in Germany

The First 24 Hours for Foreign Companies
and Their Directors

*By Philipp Busse, Criminal Defense Lawyer,
Schlun & Elseven Rechtsanwälte*

Who Should Read This Guide?

Foreign companies with operations in Germany, their directors and executives, in-house counsel, and foreign law firms advising clients with German business interests who need to understand how to respond if investigators arrive.

Key situations covered

- ✓ Search of business premises by German prosecutors, police, or tax investigators
- ✓ Digital seizures and IT system access during a search
- ✓ Employee interviews during an investigation
- ✓ The post-search phase and internal investigations
- ✓ Coordination between foreign general counsel and German criminal defense counsel

Introduction

A dawn raid by German prosecutors, police, or tax investigators is one of the most disorienting situations a foreign company and its directors can face. Investigators arrive without warning, often early in the morning, armed with a search warrant and authority to seize documents, devices, and data. For directors and employees unfamiliar with German criminal procedure, the instinct to cooperate fully - to answer questions, hand over files, and demonstrate good faith - can cause serious and irreversible legal damage within the first hour.

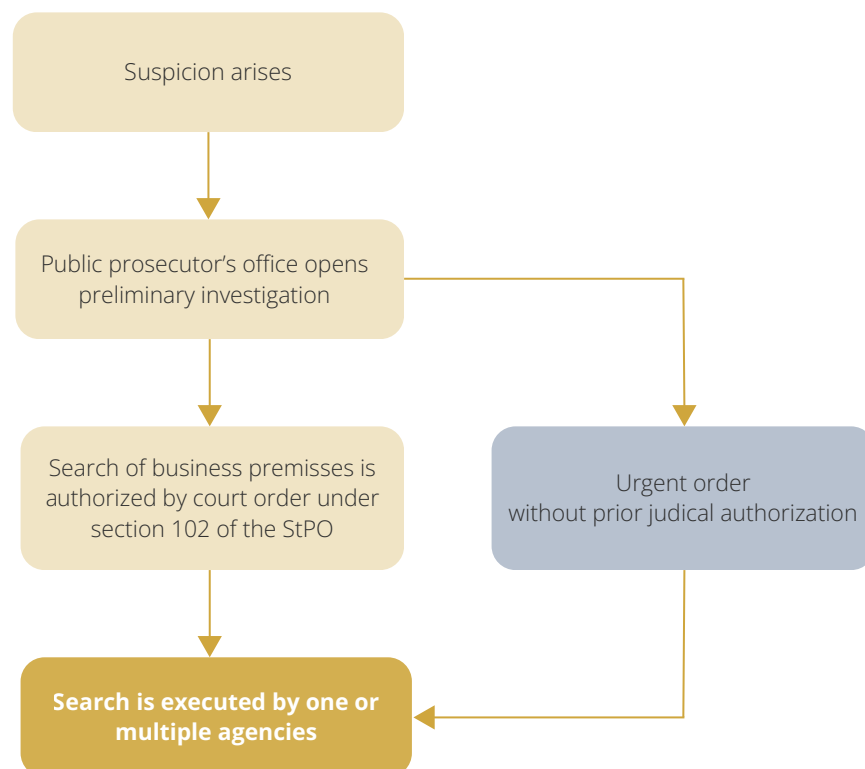
This article sets out what foreign companies and their directors need to know before, during, and immediately after a search of business premises in Germany. The decisions made in the first 24 hours frequently determine the legal and reputational outcomes that follow.

1. How Dawn Raids Begin in Germany

Business crime investigations in Germany rarely begin with a formal charge or arrest. The triggers are often less visible: a routine tax audit that flags an irregularity, a report from a whistleblower, a tip from a foreign authority, or a co-suspect in a separate investigation who names individuals at the company. Once a suspicion arises, the public prosecutor's office (Staatsanwaltschaft) opens a preliminary investigation, which can last for months before the company or its officers are formally notified.

A search of business premises is authorized by court order under Section 102 of the German Code of Criminal Procedure (Strafprozessordnung - StPO), typically issued by the investigating judge at the request of the prosecutor. In cases of urgency, the prosecutor may order a search without prior judicial authorization - but this carries its own procedural requirements and is subject to judicial review.

The executing authority may be the criminal police (Kriminalpolizei), the tax investigation service (Steuerfahndung), customs investigators (Zollfahndung), or a combination of agencies. Each operates under its own statutory framework, but the immediate practical situation for the company and its personnel is similar: investigators arrive on site with authority to search and seize.



2. The First Minutes – What To Do Immediately

The first minutes of a dawn raid set the tone for everything that follows. The following steps should be taken as soon as investigators arrive:

Remain calm and do not obstruct. Resistance is not legally permissible once investigators hold a valid warrant and will achieve nothing other than aggravating the situation. Instruct all staff to remain calm and professional.

Request to see the search warrant. The company has the right to inspect the warrant and obtain a copy. This is not obstruction - it is a legal right and an essential first step. The warrant defines the precise scope of the investigation: what offenses are alleged, which premises are covered, and what categories of documents or data investigators are authorized to seize. Investigators do not have a blank check. The warrant defines their authority, and anything seized outside its scope is legally contestable.

Identify who is in charge. Establish which authority is conducting the search and the name and contact details of the lead investigator. This information is essential for your lawyers.

Contact German criminal defense counsel immediately. This is the single most important step in the first minutes. You have the right to contact a lawyer at any point during a search. Do not wait until the search is concluded. German criminal defense counsel can advise in real time, attend the premises, review the warrant, monitor the investigators' conduct, and ensure that legally protected materials are not seized. If the company does not yet have German criminal defense counsel, this must be arranged without delay.

Notify foreign general counsel. Where the company has in-house or external counsel abroad, they should be notified immediately. However, foreign counsel cannot substitute for admitted German criminal defense lawyers in German proceedings, and coordination between the two should be established from the outset.

Do not make any spontaneous statements. No director, manager, or employee should answer investigators' questions, provide explanations, or volunteer information before consulting with counsel. The right to silence applies in full. This is not a sign of guilt - it is a fundamental procedural right that experienced investigators expect to be exercised.

3. Managing the Search – Document Seizures and IT Access

Once the search is underway, the company's primary task is to monitor what is happening and ensure that investigators act within the scope of the warrant.

Do not leave investigators unattended. A company representative - ideally accompanied by German counsel as soon as they arrive - should accompany investigators throughout the premises. This is permitted and advisable. It allows the company to observe and record what is being seized, identify any items that may fall outside the warrant's scope, and raise objections in real time where necessary.

Record everything. Keep a detailed log of the search: when it began, which rooms were accessed, which files, devices, or physical items were seized, and any statements made by investigators or staff. This contemporaneous record is critical for the subsequent legal review of the search's legality.

Object to seizures outside the warrant's scope - but do not physically obstruct. Where investigators attempt to seize items that appear to fall outside the authorized scope, the company's representative should formally object and note the objection for the record. The objection is then addressed through the courts after the search. Physical resistance to seizure is not the appropriate response and can constitute a criminal offense in itself.

IT systems and digital data. Investigators increasingly target IT systems, email servers, and mobile devices. They are authorized to access and copy data within the warrant's scope. Companies should ensure that an IT representative or third-party specialist is available to assist with - and monitor - digital seizures. Where cloud-based systems or servers located outside Germany are involved, the cross-border dimension requires immediate attention: the legal basis for accessing data stored abroad is a distinct issue that German counsel should address in real time.

There is no obligation to provide passwords, PINs, or access credentials to investigators. Employees should be instructed not to volunteer this information. In certain cases - for example, where a lawyer's device contains confidential client data protected by professional privilege - there may be a positive obligation to object to the seizure rather than simply declining to assist. The appropriate response depends on the nature of the business and the data involved, and German counsel should be consulted immediately.

IMPORTANT NOTE

Do not provide passwords or PINs to investigators. There is no legal obligation to do so. Where devices contain privileged or confidential client data, objecting to seizure may not only be permitted but required. Note the objection formally in the search protocol and contact German criminal defense counsel immediately.

Do not delete data. Under no circumstances should documents, emails, or data be deleted once it becomes apparent that investigators are present or that a search is imminent. Destruction of evidence is a criminal offense under German law and can transform an investigation into a significantly more serious matter.

4. Legal Privilege – What Is Protected and What Is Not

Legal professional privilege is one of the most practically significant issues in any dawn raid, and one that foreign companies frequently mishandle due to unfamiliarity with how German law treats it.

Under Section 97 StPO, documents and communications that fall within the scope of professional secrecy - notably correspondence between the company and its external German defense counsel - are protected from seizure. Investigators are not entitled to seize documents covered by this privilege.

However, German law draws important distinctions that foreign companies must understand:

External defense counsel correspondence is protected. Written and electronic communications between the company and its admitted German criminal defense lawyers are privileged and cannot be seized.

In-house counsel correspondence is generally not protected. Unlike in many common law jurisdictions, communications with in-house lawyers in Germany do not attract the same privilege as communications with external counsel. This is a critical difference from US and UK practice that regularly catches foreign companies off guard.

IMPORTANT NOTE

Foreign companies accustomed to US or UK privilege rules should assume that communications with in-house lawyers are not protected from seizure in Germany. Sensitive internal communications on matters under investigation should be routed through external German criminal defense counsel where possible.

Internal investigation reports may not be fully protected. The privilege status of internal investigation reports prepared by external lawyers is a complex and contested area of German law. The position depends on the specific circumstances and how the report was commissioned and used.

Where investigators attempt to seize privileged materials, the company's German counsel should raise a formal objection immediately. Privileged items should be placed in a sealed envelope and submitted to the court for review rather than released directly to the prosecutor.

5. Employee Interviews During the Search

Investigators conducting a dawn raid may seek to interview employees on the premises. Foreign companies must understand both what investigators are entitled to do and what employees are entitled to refuse.

Employees have the right to remain silent. Any employee who may be a suspect - directly or peripherally - in the investigation has the right under German law not to make any statement that could incriminate them. This right exists regardless of their formal status in the proceedings. Employees should be advised of this right before investigators arrive, ideally as part of the company's crisis response procedures.

Witnesses are generally required to testify, but even a witness cannot be compelled to answer questions that would incriminate them personally. If a witness interview begins to move in a direction that creates personal exposure, the individual has the right to decline to answer specific questions.

Works council members. Employees have the right to request the presence of a works council (Betriebsrat) member during an interview conducted on company premises. This right should be communicated to staff.

Do not coordinate employee statements. Any attempt by management to align or coordinate employee statements before or during interviews can constitute obstruction of justice or related offenses under German criminal law. Each employee should be advised individually to exercise their right to silence and to seek legal advice before making any statement.

6. Tax Authority Searches – Specific Considerations

Where the search is conducted by the Steuerfahndung - the tax investigation service - rather than the criminal police, the same fundamental principles apply, but with some additional considerations.

Tax searches are authorized under Section 208 of the German Fiscal Code (Abgabenordnung - AO) and typically arise from suspected tax evasion, irregularities identified during a routine audit, or information received from foreign tax authorities under international exchange-of-information arrangements.

A critical practical point: once a tax investigation has been formally opened, it is no longer possible to file a voluntary self-disclosure (Selbstanzeige) that would extinguish criminal liability. Any opportunity for a self-disclosure is lost from the moment the investigation commences. Foreign companies that have identified tax compliance issues should seek immediate advice on whether a self-disclosure might be appropriate before any investigation is initiated.

IMPORTANT NOTE

The window for voluntary self-disclosure closes the moment a formal tax investigation begins. Once investigators arrive, that option is gone. Companies aware of potential tax exposure should take urgent legal advice before any investigation is opened.

During a tax search, the same rules on silence, document seizure, privilege, and monitoring of investigators apply as in a criminal police search. The investigators should be treated professionally, but no information should be volunteered without prior legal advice.

7. Internal Investigations and the Post-Search Phase

The period immediately following a dawn raid is as legally significant as the raid itself. The following steps should be initiated without delay.

Conduct an immediate legal assessment. German criminal defense counsel should review the search warrant, seizure records, and search log to assess whether investigators acted within their authorized scope and whether any legally protected materials were seized. Where irregularities are identified, the basis for challenging the search before the courts should be evaluated promptly.

Preserve all remaining evidence. Materials not seized by investigators should be preserved and secured. Any destruction of remaining documents or data at this stage carries serious legal risk.

Initiate an internal investigation. Depending on the nature of the allegations indicated by the warrant, the company should consider commissioning a structured internal investigation to establish the facts before prosecutors build their case. A professionally conducted internal investigation - led by external counsel and conducted in compliance with German employment law, data protection law, and criminal procedure - allows the company to understand its exposure, take corrective action where necessary, and demonstrate to regulators that it is taking the matter seriously. Internal investigations conducted carelessly, or in a way that interferes with ongoing criminal proceedings, can, however, create additional legal problems. External counsel should lead this process from the outset.

Crisis communications. A dawn raid may become public. Employees, clients, and business partners will have questions. Any public statement must be carefully reviewed from a legal perspective before it is made: statements that are inconsistent with the company's legal position in the investigation, or that reveal information that should remain confidential, can cause serious damage. German counsel should advise on what can and cannot be said, and when.

Coordinate with foreign general counsel. Where the company has parallel legal exposure in other jurisdictions - through related proceedings abroad, cross-border regulatory requirements, or group-level reporting obligations - the coordination between German criminal defense counsel and foreign general counsel is essential. Statements made in one jurisdiction can have consequences in another, and the sequencing of disclosures must be managed carefully.

8. Common Mistakes

- 01 Cooperating without counsel present.**

The instinct to demonstrate good faith by answering questions and providing documents without legal representation is one of the most damaging errors a company can make. Investigators are professionals. Spontaneous statements, however well-intentioned, regularly create evidentiary problems that cannot be undone.
- 02 Assuming in-house counsel communications are privileged.**

As noted above, communications with in-house lawyers do not attract privilege in Germany to the same extent as in many common-law jurisdictions. Foreign companies that have shared sensitive internal communications with in-house counsel are often surprised to discover that those communications may be seized.
- 03 Failing to monitor digital seizures.**

Companies that allow investigators to access IT systems without supervision or with no specialist present lose the opportunity to object to seizures outside the warrant's scope and fail to build the record needed for a subsequent legal challenge.
- 04 Coordinating employee statements.**

Any attempt to coordinate or align what employees will say to investigators is legally dangerous and can constitute a separate criminal offense. Each employee should receive individual advice on their right to remain silent.
- 05 Deleting data.**

Deletion of documents or data once an investigation is underway or suspected is a criminal offense in Germany. The temptation to clean up compliance problems before investigators find them must be firmly resisted.
- 06 Underestimating the speed of German proceedings.**

German prosecutors and courts move quickly. The period between a search and formal charges being brought can be short. Companies that delay in retaining German criminal defense counsel find that the window for influencing the trajectory of the investigation has already narrowed significantly by the time they act.

9. Key Takeaways

- ✓ A dawn raid by German investigators typically follows a period of preliminary investigation that the company was unaware of. The raid is rarely the beginning of the case.

- ✓ The company has the right to inspect the search warrant. Investigators' authority is defined by its scope. Items seized outside that scope are legally contestable.

- ✓ Contact German criminal defense counsel immediately. The right to legal representation applies from the first moment of the search and should be exercised without delay.

- ✓ No director or employee should make any statement to investigators without prior legal advice. The right to silence applies in full.

- ✓ In-house counsel communications are generally not privileged in Germany. Correspondence with external German defense counsel is protected.

- ✓ Do not delete documents or data once an investigation is underway or suspected. Destruction of evidence is a criminal offense.

- ✓ Internal investigations, where appropriate, should be led by external counsel and conducted in compliance with German employment, data protection, and criminal procedure law.

- ✓ Foreign lead counsel and German extradition counsel must coordinate from the outset. Foreign general counsel and German criminal defense lawyers must coordinate from the outset. Statements and disclosures across jurisdictions must be managed carefully.

- ✓ Early intervention by experienced German criminal defense counsel is the single most effective way to manage legal and reputational risk in the first 24 hours and beyond.

Criminal Defense Practice Group



LEAD CONTACT

Philipp Busse - Criminal Defense Lawyer

Business Criminal Law | Cybercrime | Extradition Law

Former public prosecutor at the Cologne Public Prosecutor's Office. Advises and represents companies and executives facing criminal investigations, premises searches, and asset seizure proceedings in Germany.

SUPPORTING TEAM



Thorsten Weckenbrock Criminal Defense Lawyer

*Business Criminal Law |
Cybercrime | Extradition Law*



Josefine Roderigo, LL.M. Criminal Defense Lawyer

*Criminal Defense | Forensic
Psychology | Extradition Law*

CONTACT



E-Mail
info@se-legal.de



Phone
+49 221 93295960

Schlun & Elseven Rechtsanwälte PartG mbB
Bayenthalgürtel 23, 50968 Cologne, Germany

se-legal.de

