contrast



The knock is still at dawn, the search is digital. The digital dawn raid.

Imagine...

You are the CEO of a company that designs and installs professional sound and lighting systems for music festivals and live events. Spring is when everything accelerates. Contracts are signed, crews are scheduled, equipment is tested. After months of preparation, the festival season is about to start.

All is well… and then one morning, your day has barely started, your receptionist tells you to come to the reception, immediately.

Police officers are standing there, together with officials from a competition authority. They hand you a search warrant and explain that they are conducting an unannounced inspection in a competition investigation.

You start scanning the first page and feel a small panic rise: *this cannot be happening*. Before you finish the second paragraph, the questions land: Can you explain how your IT environment works? Can you grant us access to it? Do employees use personal devices for work? Someone else mentions a legal hold.

Your mind shifts into a mental checklist, but instead of clarity, it only raises new questions: Who do you call first? Who understands our IT environment and who can grant access?

How does this work exactly, and what are you supposed to do now?

A brief clarification.

A central task of any competition authority is to enforce compliance with the competition rules and, where appropriate, to establish infringements and impose sanctions. One of the tools available for that purpose is the so-called dawn raid: an unannounced inspection aimed at investigating whether serious suspicions of anti?competitive conduct are justified. Those suspicions often arise from complaints or leniency applications. An authority can also start an investigation at its own initiative. The Belgian Competition Authority, for example, has recently conducted dawn raids in the road signage and street furniture sector following a screening of publicly available information.

Not only the way dawn raids are triggered has become more digital, but also the way they are conducted. Where dawn raids once focused on searching filing cabinets, physical files and company cars, today's inspections are mainly digital.

Inspectors may examine a company's entire IT environment, including cloud services, servers, desktop computers, laptops, tablets, and other mobile devices, even where those are private devices used for professional purposes (BYOD). This includes access to business communications such as emails, collaboration- and messaging platforms, as well as AI chatbots.

A digital search is not a superficial exercise. Inspectors use forensic IT tools to run keyword searches across large datasets and create digital copies of electronic data for further review, often at the authority's premises.

Companies have a duty to cooperate fully with dawn raids. Refusing to cooperate, or doing so only partially, can have grave consequences. In practice, this often places IT at the centre of the inspection. IT teams may be asked to explain how systems and data flows are organised, or to execute specific technical requests such as temporarily blocking individual user accounts, temporarily disconnecting running computers from the network or providing administrator access rights support.

The message is clear: a modern dawn raid is both a legal issue and an IT issue.

Concretely.

- **Preparation is crucial.** Ensure that you have an up?to?date dawn raid protocol in place. Include a detailed IT section that, among other things, maps key systems and data locations (on?premises and in the cloud), identifies who can grant access rights, and sets out how legal holds (ensuring that no data can be deleted or altered) and data exports work. You do not want to be figuring this out on the day of a dawn raid. Train your IT staff.
- **React calmly and immediately when inspectors arrive.** Ask to read the search warrant. Verify the identity of the inspectors and check what the precise object and scope of the investigation are. Request legal assistance and involve the responsible IT contact straight away.
- **Avoid obstruction.** Cooperate fully and professionally. Under no circumstances should you move, conceal, remove, or delete documents or data. Be aware that obstruction may also result from technical mishaps: delayed, incorrect, or uncoordinated IT actions during an inspection, may be qualified as obstruction. The European Commission has imposed 2.5 million euros in fines for failing to block an email address and diverting incoming emails.
- **Seek clarity and avoid assumptions.** If a request is unclear, ask for clarification. If you need time to

execute a technical request safely, say so.

- **Document the raid yourself.** Keep an internal log of what is requested, which systems are accessed, which searches are run, and which data is copied or reviewed.
- **Monitor for dawn raids at competitors, suppliers, or customers.** If your competitors, suppliers, or customers are subjected to a dawn raid and you are not, this does not mean you are off the radar of the competition authority. Evidence collected in dawn raids at other companies may be used against you as well. It is therefore advisable to monitor the websites of competition authorities for dawn raids that may affect you.

Want to know more?

- Would you like to know more about searches by the European Commission? See the Explanatory note on Commission inspections.
- Would you like to know more about searches by the Belgian Competition Authority? See the Guidelines of the Belgian Competition Authorities concerning dawn raids.
- **contrast** organises workshops where the participants are guided step by step through the different stages of a dawn raid and a concrete action plan is discussed. Don´t hesitate to contact us for more information: compliance@contrast.law.
- In the Picture October 2021. Ready for a (home) search by the competition authority?

Authors

Michèle de Clerck