WARDYŃSKI & PARTNERS

Dawn raid policy

why your company should consider adopting one

MAY 2020

KEY INFORMATION

What is a dawn raid?

A dawn raid is an unannounced inspection of a company's premises, usually as part of an ongoing investigation by regulatory or law-enforcement authorities.

Any company, no matter its size, may be subject to a dawn raid. Dawn raids are usually triggered by a complaint (e.g. from a customer or distributor), an anonymous tip, or a leniency application. They may also be initiated by authorities with their own agenda.

In Poland, different authorities are vested with powers to inspect business premises. The prospect of having any particular authority ring your doorbell generally depends on the type of business you run. Most businesses may be inspected by law-enforcement and tax authorities, social-insurance authorities, labour inspectorates, data protection authorities, and competition and consumer authorities. Those engaged in more specialised activities, in particular under certain licences, may also be subject to inspection by a specialised agency (such as the National Sanitary Inspectorate, the Trade Inspectorate, the Environmental Protection Inspectorate, the Border Guard, or the Financial Supervision Authority).

The exact powers of these agencies differ. Their powers may also be specified in the particular warrant granted to the agents. At their most extensive, these powers allow authorities to enter premises, search and seize documents and electronic files, and seize equipment (e.g. computers or hard drives). They may also include interviewing employees and even sealing off rooms.

No doubt a surprise dawn raid would cause disruption. But proper preparedness will mitigate the risk of mistakes and may contribute to making the entire process less troubling.

What is a dawn raid policy?

There are several things that can go wrong at the start and during the inspection. The purpose of a dawn raid policy is to design a clear and simple procedure for how staff should behave, especially those on the front line of the inspection: reception and security.

There is no one-size-fits-all policy. It should be specific to your organisation. In general a dawn raid policy will address the following issues:

1. Arrival of investigators

Reception and security staff need to have clear instructions what to do when approached by investigators. The policy will usually specify that the investigators should be allowed to enter the site, but the reception staff should kindly request them to wait for people with appropriate authority to assist them further

2. Scrutinising the warrant

The policy will usually specify the persons in charge of verifying the warrant and identity documents of the investigators.

3. Notifying management

The reception and security staff should be aware that they need to notify the designated management of the dawn raid. They should have current direct contact details to the designated management and keep trying to reach them until successful. The policy may specify the order of contact and the means of communication.

4. Assembling a coordination team

The policy will usually describe who at the company should become part of the dawn raid coordination team. Most commonly, the coordination

team includes senior management, in-house lawyers, IT staff, and external lawyers. As not all members of the coordination team are likely to be on-site and may need time to get to the premises, it is essential that an emergency coordinator always be present at each of the company's premises. That person should handle the investigators until the coordination team is present on site.

5. IT

As the vast majority of documents are stored only electronically, the company needs to identify who from the IT staff has sufficient knowledge and administrator's rights to assist in the raid. If those persons are located offsite, it is necessary to have their direct contact details. It is important to notify the designated IT person of the dawn raid. That person may need to assist the investigators in their search, and often in sifting through electronic files. IT staff should also secure copies of electronic documents. All routine document destruction procedures should be suspended for the duration of the dawn raid.

6. Managing employees

The policy will usually advise to inform employees of the inspection. The staff should also be instructed not to destroy or conceal any documents or electronic files. It is forbidden to discuss testimony or mislead officers. The employees should be advised that they should cooperate, but not volunteer any materials. They should be aware of their rights and know whether and when they can remain silent. They should also be aware whether they may request the presence of a lawyer. It is important to instruct every staff member not to sign any reports or declarations not accurately reflecting the full content of their interview.

7. Kontrola działań funkcjonariuszy

If possible, each inspector should be accompanied by a "shadow" staff member or external lawyer. The shadow is there to ensure that the inspectors do not exceed their powers. They will usually keep a record of all documents reviewed, all questions asked, and all employees interviewed. They will also make sure that privileged materials are handled properly.

The dawn raid policy may also go beyond mere instructions on how to handle the inspection. It can put in place procedures for how documents and electronic files are to be stored and copied. This especially concerns privileged documents. These should be clearly marked and stored in one place everyone would know. A comprehensive dawn raid policy should also cover the issue of data backup. If for example hard drives are taken by the investigators, the company has to have its data secured so it can resume operations after the investigation.

The list of issues that can be covered by the policy is open-ended, and depends on the nature of the company's business.

Is the policy enough?

The answer is simple: a policy is not enough. It must be well known within the organisation, in particular among the first responders (reception, security and IT staff, in-house lawyers).

The policy must be up to date. An outdated policy known to a few will not be fit for purpose, and may do more harm than good.

Hence it is essential to make sure that all employees are aware of the policy, and preferably receive training on the policy. However, even the best training in a cosy conference room will fall far short of a realistic drill. A drill will not only help train staff, but also assist in testing the organisation's preparedness.

Last but not least, even the best policy and trained staff may not be enough. No matter how well trained, staff will be under stress and may be intimidated by the horde of investigators. During the inspection, many issues may pop up with no easy answers: whether the company must provide access to encrypted documents, whether the company needs to turn over cloud-stored files on servers in foreign jurisdictions, etc. Hence it is best to consider having emergency contacts to lawyers with experience handling dawn raids and related proceedings. Raids are often conducted outside office hours (e.g. very early in the morning), so it is good to have trusted advisers who are available 24/7.

Team

Łukasz Lasek
adwokat, partner
lukasz.lasek@wardynski.com.pl

Antoni Bolecki
radca prawny, wspólnik
antoni.bolecki@wardynski.com.pl

Szymon Kubiak
radca prawny, wspólnik
szymon.kubiaki@wardynski.com.pl

Michał Nowacki
radca prawny, doradca podatkowy, wspólnik
michal.nowacki@wardynski.com.pl

Krzysztof Wojdyo
adwokat partner
krzysztof.wojdylo@wardynski.com.pl