arendt

LUXEMBOURG

Dawn raids and inspections be prepared

arendt.com

Introduction

Economic and financial regulations are increasing in number and complexity. The staff and material resources of the administrative and judicial authorities are growing. Prosecution policy is to target economic crime. Virtually every new law in this area introduces new offences or administrative sanctions and extends into new fields, such as ESG and whistleblowing.

Being subject to an administrative audit or a police search is not a hypothetical scenario, it is a concrete risk to which every business is exposed. Even though the relevant authority leads the operation, if you are prepared and have clear procedures in place, you can retain some control over the process. If a business is unprepared, there is a risk of panic and disorganisation on the day, which can have negative consequences that are difficult to remedy afterwards. The matter will start off on the wrong track, right from the outset.

This mini-guide aims to give a general overview of the rules on searches and administrative audits, together with practical advice on how to prepare for and manage these situations.

This guide is a summary of the main rules applicable and does not replace the need for analysis and legal advice on a case-by-case basis. If you require such analysis or legal advice, Arendt's lawyers and experts are at your disposal.

Table of contents

Fundamentals

Q1 : What is the difference between a search and an inspection (investigation/audit)?

Searches (*perquisitions)* are ordered and conducted by the judicial authorities: the investigating judge *(juge d'instruction)*, the public prosecutor *(procureur d'Etat)* and police officers (*officiers de police judiciaire)*.

Their purpose is to establish the facts constituting a criminal offence and, in particular, to collect evidence aimed at securing a criminal conviction (fine or imprisonment).

Example: the police conduct a search to trace the movement of funds related to an internet scam.

Inspections, also known as investigations or audits *(enquêtes/contrôles)*, are carried out by other Luxembourg authorities, such as government departments, supervisory authorities, and self-regulation bodies. Their purpose is to verify that the business has complied with specific legislation or regulation. A finding of non-compliance may lead to an administrative sanction, and, in certain cases, criminal proceedings.

Example: the Commission de Surveillance du Secteur Financier (CSSF) checks whether a regulated entity is complying with anti-money laundering and anti-terrorist financing obligations.

Q2 : Who can be targeted by these measures?

In the case of on-site inspections, it is always the business itself, and sometimes individual managers, who are audited and possibly sanctioned.

Example: the CNPD *(Commission nationale pour la protection des données)* checks whether a business is complying with data protection rules. If it observes any shortcomings, it may decide to impose an administrative fine.

Criminal searches may target a third party. Therefore, the business may simply be the place where the police look for evidence of offences committed by the third party.

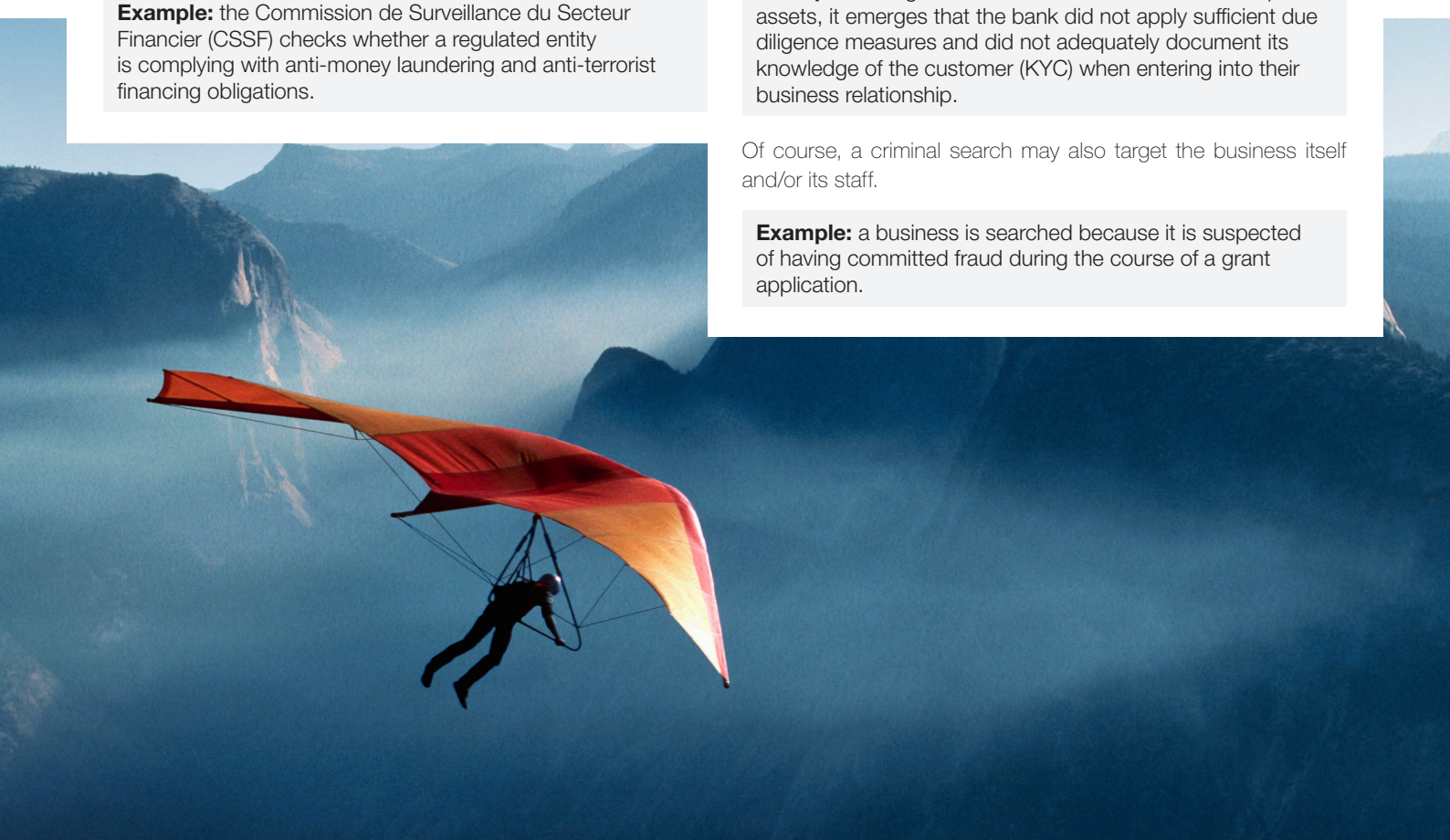
Example: the police search a bank for information about the alleged misuse of corporate assets by or belonging to one of the bank's clients.

Even if the search relates to a third party, the police may find incriminating evidence against the business which may lead to proceedings being opened against the business.

Example: during a search related to the misuse of corporate assets, it emerges that the bank did not apply sufficient due diligence measures and did not adequately document its knowledge of the customer (KYC) when entering into their business relationship.

Of course, a criminal search may also target the business itself and/or its staff.

Example: a business is searched because it is suspected of having committed fraud during the course of a grant application.



Searches and seizures

Q3: Is advance notice given for searches?

Searches do not have to be notified in advance. As a rule, they are not and the police may turn up at a business at any time.

Sometimes, when the police are expecting the person subject to the search to cooperate, they may notify and prepare for the search in advance, for example by sending an email. This is most often, if not exclusively, the case in situations where the business itself is not the target of the investigation giving rise to the search, but rather a third party.

Q4: When can a search take place?

Unless a crime is being committed, a search cannot start before 6:30 am or after midnight.

Usually, searches of businesses are conducted on working days and start during office hours.

Q5: How long does a search last?

Depending on what is sought and how quickly the information is collected, a search may only last a few hours, or it may go on until late in the evening, or even last several days.

Q6: Do the police always come to the site?

In principle, the police officers come to the locations being searched.

However, a recently adopted law makes permanent a system introduced during the COVID-19 pandemic, under which the police may notify the search order by email. In practice, email notification will only take place in cases where a third party, rather than the business itself, is the target of the investigation giving rise to the search, and there is no risk of evidence being lost.

There are specific rules obliging banks to provide information on request about accounts opened with them. These communications will normally take place via email.

Q7: Does the business have to cooperate with the police?

In principle, no one is obliged to cooperate actively with a search. The business has the right to remain silent and not incriminate itself.

Nonetheless, the police officers may search the business and look for the documents and data in question themselves, which can be very disruptive to the business' operations.

Other than in specific cases, it is therefore preferable to assist the police with their search.

Obstructing the work of the police is prohibited in any circumstances.

Under a law adopted in July 2023, the police are able to notify search orders by email and the recipient is obliged to cooperate. However, this procedure cannot be used if the recipient is suspected of being a perpetrator of, or accomplice to, the offences in question.

In the case of administrative inspections, certain regulated entities have a general duty to cooperate with the authorities and to respond to any lawful request made by law enforcement authorities in the exercise of their powers.

Q8: Who can conduct a search?

In principle, one or more police officers conduct the search, possibly assisted by other police staff and certain specialists, such as IT experts.

In international mutual assistance cases, Luxembourg police officers may be accompanied by their foreign colleagues.

Representatives from the public prosecutor's office or even the investigating judge may also be present. However, this rarely happens in practice, other than in very complex and large-scale cases.

Q9: What are the requirements for a lawful search?

The police do not have unlimited authority to conduct a search or seize property.

Unless a crime is under way, search and seizure may only be carried out by order of the investigating judge. A copy of the order is served (delivered), usually before the search operations begin.

The order indicates the locations which may be searched, and the objects and documents sought. Only documents and evidence covered by the order may be seized.

Q10: In what context can a search take place?

The judicial authorities can act in any area covered by the criminal law, which has an extremely broad scope. This includes:

- Fraud, deception, theft, and embezzlement
- Money laundering
- Failure to comply with anti-money laundering obligations
- Computer crime (cybercrime)
- Corruption
- Tax offences

Any offence *(délit or crime)* may give rise to a search, regardless of the level of seriousness.

Q11: What is the purpose of seizure?

The primary purpose of seizure is to collect evidence relating to an offence, either incriminating or exonerating.

Example: the police seize the accounts of a business.

However, a seizure may also take place with a view to the subsequent confiscation of anything forming the object or proceeds of the offence.

Example: the police seize a bank account balance because it derives from the misuse of corporate assets.

The law also provides for seizure of equivalent assets *(saisie par équivalent)*, which does not require any link between the offence and the property seized.

Example: if the investigation concerns fraud of EUR 200,000 but the money cannot be located, the police may seize a flat belonging to the suspect.

Q12: How are seized assets stored?

In principle, seized assets are deposited with the judicial authorities. Data is usually stored on police servers or in digital format added to the case file.

The rules were modernised in 2022 and the Asset Management Office (*Bureau de gestion des avoirs*) was created. It is able to look after assets that require management, such as buildings. Assets seized from bank accounts and other receivables are, as a rule, transferred to the State Consignment Office *(Caisse de consignation)*. Perishable goods can be sold, and worthless goods destroyed.

Any affected person may also request that an asset is sold if retaining it risks a significant depreciation in value or the retention costs are disproportionate.

Q13: What happens to seized property?

Objects seized as evidence become an integral part of the case file, as exhibits.

Confiscation means that the property is transferred to the State. Certain merchandise is destroyed, such as counterfeit goods. Valuable items may also be used to provide compensation to parties claiming damages (*parties civiles*).

Other goods may be:

- Returned during the investigation or inquiry, either spontaneously or on request.
- Returned at the end of the proceedings, in the case of a discharge or an acquittal.
- Confiscated if the proceedings result in a conviction or returned to the victim of the crime.
- Under certain conditions, confiscated despite a discharge or an acquittal.

Q14: What powers do police officers have?

The police have the right to enter the premises, search/inspect them and seize any documents, objects and data covered by the search order.

Resisting police action is an offence and the police can use force if necessary.

In practice, however, a search of business premises usually proceeds calmly and with the cooperation of the business, in order to locate the relevant documents and avoid excessive disruption to the business.

Q15: How are documents seized?

The police can seize the originals or take copies instead.

Q16: How is electronic data seized?

In principle, the police have the option to either seize the computer medium on which the data is stored or seize the data directly.

When seizing from a business, the police usually take copies and the business retains its data. However, if using the data is illegal or threatens the safety of people or property, it can be removed from the business.

If the dataset is too large to review and analyse for relevance on the day of the seizure, a so-called "general" seizure may take place. The data copied is placed in full under the administration of the court, to be indexed and sorted at a later date. At this stage, the data cannot be used either to incriminate or exonerate. For the time being, this mechanism is not set out in law, so it presupposes the agreement of the business.

Q17: Can a search and seizure be challenged?

To the extent that the police act within the limits of the seizure order, the business must acquiesce to their intervention and to the seizure.

However, in a domestic (Luxembourg) procedure, any person concerned who has a legitimate personal interest may lodge an application to set aside within 5 working days of becoming aware of the measure. The application can be directed towards the order and/or the search itself. This remedy allows procedural irregularities to be raised. However, the court will not review the exercise of the discretion to prosecute or to conduct the search.
In international mutual assistance cases, a district court judge in chambers automatically reviews the lawfulness of the proceedings. In any event, any person concerned who can demonstrate a legitimate personal interest may file a memorandum of objection with the court within 10 calendar days of notification of the measure to the person against whom the order is executable.

It is also possible to request the return of seized goods at any time.

Q18: Can the police speak to people as witnesses?

In principle, the purpose of a search is to look for material evidence and not to speak with people. There is no obligation to make statements to the police.

In practice, it is not uncommon for the official report *(procès-verbal)* of the search to contain information provided by the persons present during the search. However, at this stage of the case, it is preferable to restrict this to technical information useful for the conduct of the search and avoid taking any position on the offences in issue.

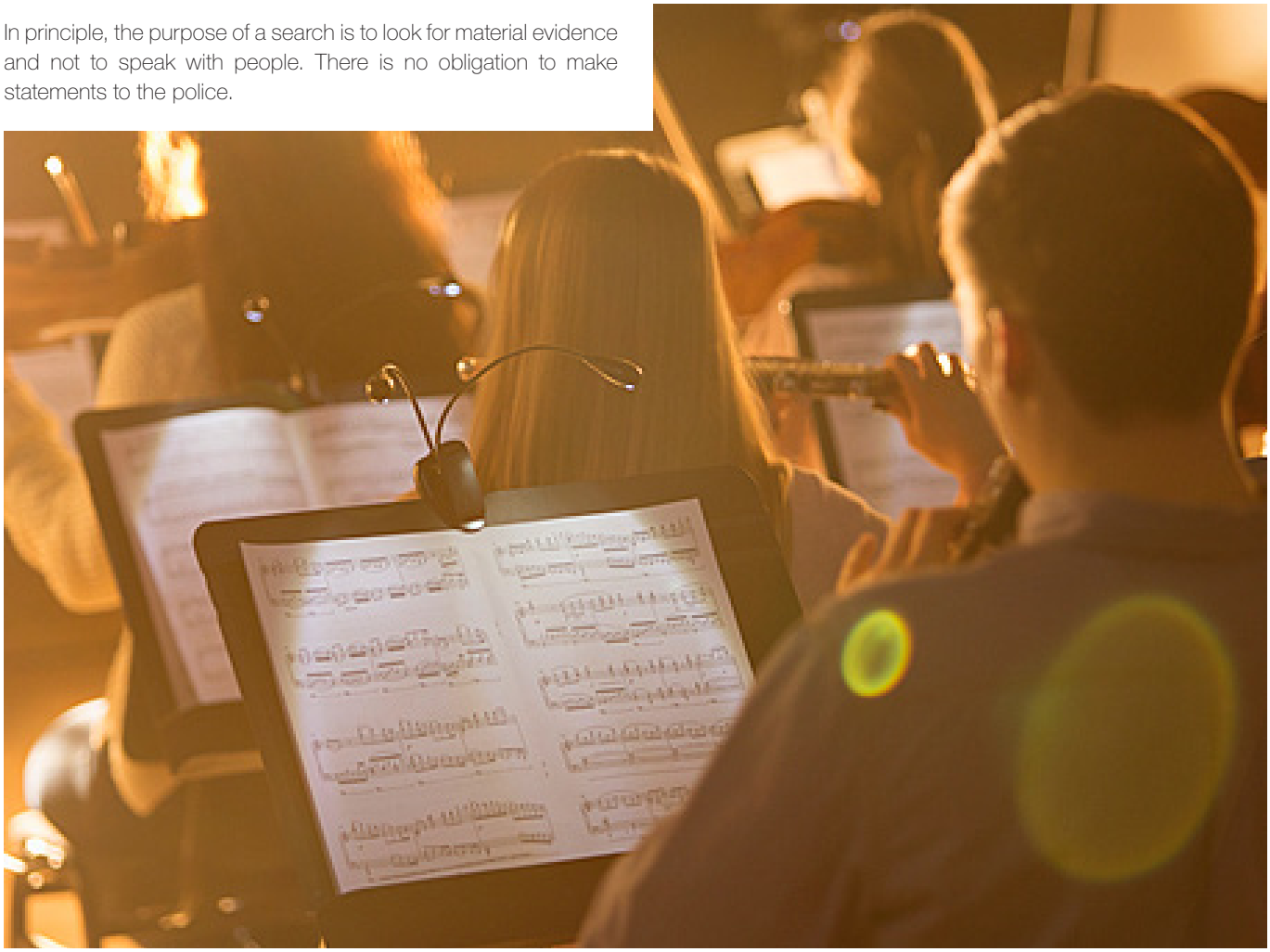
Q19: What are the formalities for search and seizure?

The search and seizure conclude with the police drawing up an official report. This should describe the operations conducted and contain an inventory of the objects seized.

It is important to ensure that the official report is complete and comprehensive as to the sequence of events and the documents and data seized (avoiding recourse to vague and generalised descriptions). In the case of a "general" seizure, the report should also set out the agreement reached about further processing of the data seized.

The police officers and the representatives of the business sign the report. If there is a refusal to sign, this is simply noted in the report.

A copy of the report is given to the business.




BZC

On-site inspections or audits

Q20 : Which authorities can conduct on-site inspections or audits?

There are numerous government departments, supervisory authorities, and self-regulation bodies in Luxembourg (the authorities) which can carry out inspections, investigations or audits within their respective fields of authority. These include:

- The CSSF *(Commission de Surveillance du Secteur Financier)*, which, in the context of its prudential supervision, has all the supervisory and investigative powers necessary for the exercise of its functions. In particular, with regard to the entities subject to its supervision, it is entitled to ensure that businesses comply with their anti-money laundering and anti-terrorist financing obligations. Its powers extend to the supervision of compliance with all regulations applicable to credit institutions and professionals of the financial sector.
- The CAA *(Commissariat aux Assurances)*, which is responsible for supervising the insurance products and activities market.
- The CNPD *(Commission nationale pour la protection des données)*, which is responsible for verifying the lawfulness of the collection, storage, use and transfer of data concerning identifiable individuals, and must ensure that their fundamental rights and freedoms, particularly their privacy, are respected in this context.
- The ITM *(Inspection du Travail et des Mines)*, which has the power to identify and put an end to breaches of legal, regulatory, administrative, and convention provisions relating to work or workplace health and safety.
- The ACD *(Administration des contributions directes)* and AED *(Administration de l'enregistrement, des domaines et de la TVA)* tax authorities, which are responsible for investigating irregularities in the declaration of direct taxes and turnover taxes, such as value added tax. It should be noted that the AED is also responsible for ensuring that certain businesses and professionals comply with their professional obligations regarding the fight against money laundering and terrorist financing.
- The ADA *(Administration des douanes et accises)*, which is responsible in particular for public health, bio-security, and safety and compliance of imported goods, and also for tax matters.
- The Competition Authority *(Autorité de la concurrence)*, which is responsible for investigating and identifying infringements of competition law which have the effect of preventing, restricting or distorting competition within the European internal market.
- The ILNAS *(Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services)*, which has a wide range of responsibilities. These include standardisation, accreditation and notification, digital trust (such as monitoring digital trust service providers and suppliers of dematerialisation and storage services), acting as the National Cybersecurity Certification Authority for the purposes of the EU Cybersecurity Act (thus overseeing and monitoring the correct application of the rules by the various players), market supervision (by verifying the conformity of non-food manufactured products for sale on the national market and carrying out tests relating to electrical safety, electromagnetic compatibility, compliance of toys and machinery, and general product safety), and product measurements.
- The ILR *(Institut Luxembourgeois de Régulation)*, which acts in the interests of consumers and ensures the proper functioning of the market on the basis of effective and sustainable competition, while guaranteeing a basic universal service. It is responsible for regulating and supervising the following economic sectors: electronic communications networks and services, electricity, natural gas, postal services and rail and air transport. It is also responsible for managing and coordinating the radio-frequency spectrum.

Certain European and overseas authorities, such as the European Banking Authority or the national supervisory authorities of other Member States or of third countries outside the EU, may also carry out inspections or audits of institutions located in Luxembourg in the context of the prudential supervision of those institutions. These authorities may conduct the audits jointly with the Luxembourg authorities or directly themselves.

Q21 : What are the rules applicable to inspections and audits?

Unlike criminal searches, which are subject to a uniform regime irrespective of the underlying subject matter, there is no single regime for on-site inspections or audits.

The conditions under which an on-site audit may take place and the documents that can be seized therefore vary, depending on the authority concerned and the type of infringements being pursued. Certain authorities, such as the CSSF, may also instruct a third party, such as an accredited business auditor or an expert, to carry out verifications or investigations at the business.

Some of these procedures are very similar to a criminal search.

Q22: Can the authority enter the premises?

Yes, in most cases, the authority concerned has the right to enter the premises under audit. Unlike for searches, the authority is not usually constrained to specific hours. For example, ITM officials can conduct an audit at any time of the day or night.

However, for practical reasons, an authority will conduct the majority of its audits during working hours.

In any situation, if an authority needs to use force, it can usually request assistance from the police.

In principle, an authority can act *ex officio* without needing a court order.

However, certain authorities, such as the Competition Authority, carry out search and seizure under court supervision.

For other authorities, such as the ITM and the ILNAS, a court application is required for an audit of residential premises.

Q23: In what situations can an authority conduct an on-site inspection or audit?

Again, it depends on the circumstances. Some authorities have the right to make random checks. For others, the law only allows them to intervene if there is evidence that a legal requirement has not been complied with.

For example, ITM officials can only carry out an audit if there is sufficient evidence or legitimate grounds to justify their intervention.

On the other hand, the ADA has the power to do random audits. In the same vein, the ACD conducts on-site audits every three years on businesses exceeding a certain turnover or profit threshold.

Q24: Who can be targeted by an on-site inspection or audit?

Other than in exceptional cases, on-site audits only target the business itself. Unlike police officers conducting a search, the authorities cannot in principle search businesses for evidence relating to third parties.

Q25: Can the authority find facts that are outside its competence?

Each authority is only competent in its own particular field.

However, if they identify criminal offences in other areas, the officials concerned are obliged to inform the public prosecutor's office. Similarly, information may be exchanged in the context of cooperation between authorities.

Q26: Are audits notified in advance?

In principle, the authorities are not obliged to notify their intervention in advance. In some cases, however, they may do so.

This is notably the case for the CSSF and the CAA, which generally inform the relevant business in writing of the purpose of the on-site inspection.

Where possible, ITM officials are required to inform the employer or its representative at the beginning of the operation. Similarly, CNPD officials are obliged to inform the manager of a business by registered letter with proof of receipt that the business will be audited. If the investigation necessitates an unannounced site visit, the authorised CNPD officials will hand over the letter on-site to the business under audit, in return for a signed acknowledgement of receipt.

Q27: Can the authority remove documents and evidence?

Every authority has different powers. Some can take away all the evidence they need, while others have powers that are limited to making on-site observations or taking samples.

For example, in the field of anti-money laundering, the CSSF and the CAA can seize any document or other item that appears useful for establishing the truth. By contrast, the ITM is generally limited to seizing documents relating to working conditions.

On-site inspections or audits

Q28: Does the business have to cooperate with the authority?

In certain procedures, for example those conducted by the CSSF, the CAA or the ITM, there is a legal obligation to cooperate.

With regard to other authorities, such as the CNPD, there is no such obligation. Nonetheless, it may be in the business' interest to cooperate in good faith, and this should be assessed on a case-by-case basis.

Q29: Can the authority speak to people as witnesses?

In principle, the authority may, depending on its area of competence, interview any person at the business concerned if an interview appears useful for establishing the truth.

Q30: What are the possible consequences of an on-site audit?

If it discovers shortcomings, the authority may initially issue a warning or a reprimand, aimed at encouraging the business to comply.

If the facts are more serious or repeated, the authority usually imposes a sanction in the form of an administrative fine or fines. In the most serious cases, the authority may also impose a temporary suspension of certain activities, or even withdraw licences, authorisations, or approvals.

It should be noted that certain authorities also have the power to impose penalties, particularly in cases of delays in compliance.

If the facts are also punishable under the criminal law, criminal proceedings may be initiated in parallel.

Q31: What remedies does the business have against these sanctions?

An authority's decision is subject to the remedies available against administrative decisions, that is, an application for variation or setting aside before the lower administrative court *(tribunal administratif)*.

In principle, a claim must be lodged within either 1 month or 3 months of notification of the contested decision, depending on the case.

Q32:

What should you do during a search, inspection, investigation or audit?

Greet the officials

The police or the representatives of the authority will usually report to the business' reception area.

Unless the search is aggressive, the judicial authorities will initially seek to cooperate with the business in a spirit of goodwill. The reception staff should make a note of the identity of the representatives, or the key personnel at least, and seat them in a meeting room.

Although great care must be taken when offering anything to public officials, it is acceptable to offer them a drink.

Reception staff can ask for the purpose of their visit in broad terms, so that they can pass on the information.

They should assure the officials/representatives that the leaders of the business have been notified and will meet with them as soon as possible.

It is therefore important and useful to train reception staff about searches, so that they do not commit any "faux-pas" on the day.

Notify business managers

The reception staff should inform the members of the leadership team as soon as possible, preferably based on a pre-established list and procedure. They should pass on any information obtained about the identity of the authority concerned and the purpose of the inquiry.

In particular, the following people should be informed:

- Senior Leadership Team
- Compliance Officer
- Head of Legal
- Head of IT
- Head of Communications

If any of these people are unavailable, their substitute should be contacted.

Depending on the situation, other people may also need to be notified. For example, in the event of an audit by the CNPD, the DPO (Data Protection Officer) must be informed. For an ITM audit, the employees' safety representative *(délégué à la sécurité)* should, as a rule, be notified.

Set up a crisis management team

It is advisable for the leaders of the business to create a crisis management team to manage the situation.

One individual should be nominated as the main contact person for the authority.

If operations are taking place at more than one location, a representative of the business should be appointed to accompany the authorities at each location.

Assess the risks

Often, the authority's intervention is just the first stage of a criminal or administrative case. The business should not be lulled into believing that everything is fine. Experience shows that irregularities are discovered in many cases, to the management team's surprise.

The risk inherent in any search or audit must therefore be assessed from the outset.

The procedure may:

- Result in a criminal conviction or an administrative sanction.
- Lead to a risk of liability to pay compensation to third parties.
- Give rise to reputational risk.
- Result in a criminal record that jeopardises existing business relationships and hinders the future development of the business, particularly by exclusion from public procurement contracts.

Q33: Who is exposed to risk?

In administrative matters, it is usually only the business that is targeted. In some cases, managers may also be liable.

In criminal matters, both the business and the individuals responsible can be prosecuted and convicted. Often, it is the managers who incur this liability. However, other employees may be prosecuted if powers have been delegated.

Instructing a lawyer

It is not compulsory to instruct a lawyer, but it is strongly recommended in most cases. The lawyer will often know the police officers or officials who are on-site, which can facilitate communication and the conduct of the inspection.

In criminal cases, there is a right to legal representation. This right is less formalised in administrative matters, but a litigant can nevertheless be represented by their lawyer in any situation.

The police and the authorities will usually agree to wait for a reasonable period to allow the lawyer to arrive on-site.

It is preferable not to sign or hand over anything nor to provide any information about the matter (verbal or written) before the lawyer arrives.

If one or more managers or employees appear to be implicated, as well as the business, it is preferable to instruct separate lawyers in most cases. This avoids conflicts of interest.

Manage the communications

Working with the Head of Communications, internal and external communication must be managed immediately.

Internally, the presence of the relevant authority is highly unlikely to go unnoticed by staff. It is best to provide some information to avoid uncertainty and false rumours. Internal communications should aim to avoid panic and remind employees of their duty of discretion. Otherwise, the search may rapidly find its way into the press or onto social media.

Externally, the first steps are to determine whether there is an obligation to inform any other authority and draft a so-called "crisis communication" to use if the information becomes public, which seeks to limit the negative consequences, particularly reputational. It may be useful to engage communications experts. Do not rush into communicating though, especially if the facts or the reasons for the search are unclear or unknown. Interaction with the press will also need to be managed carefully.

Q34: Should you involve the staff delegation?

Apart from ITM audits, there is no legal obligation to involve the staff delegation *(délégation du personnel)* during a search or audit. However, it may be useful to provide them with some information, particularly given their role in passing on information to staff.

Q35: Does the press have the right to report on what is happening?

The press must respect the presumption of innocence, which obliges it to qualify its statements. No one should be described publicly as guilty of facts that are the subject of a judicial investigation or inquiry.

The press must also balance the protection of privacy and reputation, and is subject to a duty of accuracy and truthfulness. Within these limits, the press is not forbidden from informing the public of an audit or search taking place within a business.

Q36: Does the business have to hand over confidential data?

The business cannot refuse to hand over confidential documents if they are covered by the search order or the powers of the relevant administrative authority, and they fall within the scope of the ongoing investigation/search. In Luxembourg, there is no specific mechanism to protect trade or industrial secrets.

In criminal matters, specific rules oblige the authorities to respect professional secrecy, such as banking secrecy. The court may seize documents concerning the clients under investigation, but secrecy must be preserved for any persons not under investigation, for example by redacting relevant passages. As a rule, exchanges between lawyer and client benefit from privilege, meaning that they cannot be seized.

Q37: What should you do after the seizure?

If the business is not the target of the criminal search, it is likely that they will not hear anything further about the case.

Searches targeting a business usually take place before the business is formally charged. As a result, it will not yet have access to the case file. Instead, the business will have to wait and see whether, depending on the results of the search and other evidence gathered, the authorities decide to pursue the case or drop the charges.

Q38:

How should you prepare for a search, inspection or audit?

Put the required procedures in place

To effectively manage an audit or a search, the business must be prepared and put in place the necessary procedures. It can also be useful to conduct simulation exercises on a regular basis.

Depending on the nature of the business' activity, it may be possible to identify which authorities are most likely to intervene.

In particular, the procedure should set out:

- Practical instructions for reception staff.
- List of individuals to contact.
- Members of the crisis management team which will be set up, plus their substitutes.
- Initial communications to organise.

It is also worth preparing for other issues in advance, such as the conditions under which the business will cover the defence costs of employees and managers.

Organise training and simulations

Written procedures alone are not sufficient to ensure that everything will proceed as desired in practice. It is preferable to organise training courses for the staff concerned, adapted to their positions. The training should involve practical role-playing exercises, including how to answer questions posed during a search or inspection/audit.

This training should be repeated at regular intervals, taking account of changes in personnel.

Know where to find the information

The police or the authorities will be looking for specific information. If they observe that the business does not know how to locate it quickly, this will create a bad impression from the start. Similarly, the quality and completeness of information provided to the authorities are important.

For this reason, it is useful to carry out a data-mapping exercise to gain an overview of what data the business has, where it is recorded and archived, and how it can be filtered and copied. This exercise should also include old systems that have been decommissioned, as the authorities regularly look into facts going back several years.

Q39: What should you do if the police or authorities are unable to take the desired data?

Sometimes the search order covers large volumes of electronically stored data and the officials conducting the search have neither the time nor the technical means to copy it on-site. It is not uncommon in these situations for the authorities to require the business to copy the data and hand it over within a timeframe to be agreed. In these cases, it is essential to make a so-called "forensic copy", to prove that the original data has not been altered. It is therefore preferable to use forensic technology experts to ensure that the correct process is followed and will not be challenged later by the authorities.

It is also common for the authorities to request data corresponding to certain criteria (such as keywords, time periods or individuals). It is therefore necessary to filter and sort large volumes of data. If the IT system (for example, "ShareDrive") contains several dozen terabytes of data, it will be impossible to filter it manually. Instructing forensic technology experts is becoming essential, not just for conducting the sorting exercise, but also for documenting each step. These experts will have access to specialised tools for this work.

About Business Crime, AML/CFT and Forensic Investigations, Corporate Intelligence & Litigation Support at Arendt

About Arendt's Business Crime practice area

Our business crime practice advises domestic and international clients, in particular from the banking, financial, industrial and commercial sectors at all levels, on matters including:

- Preliminary criminal risk assessments
- Avoidance of criminal risks
- Assistance during the investigation and prosecution phase, including international rogatory letters
- Negotiation of criminal settlements
- Assistance during criminal trials
- Cross-border coordination in criminal cases with international ramifications

Depending on the needs of our clients, we assist them as suspects or defendants, as victims of crime or as interested third parties.

Our team is specialised and experienced in all areas of economic, financial and banking criminal law.

Your key contact:
Jean-Luc Putz,
Partner Arendt & Medernach
jean-luc.putz@arendt.com
T +352 40 78 78 8620

About Arendt's AML/CFT practice

Money laundering and terrorism financing are threats that require constant vigilance. The pressure and regulatory scrutiny at the national and international levels is intensifying with the imposition upon companies of ever more complex global AML/CFT rules, including due to international financial sanctions. Accordingly, there has been a significant rise in supervisory activities and regulatory expectations, creating a zero-tolerance environment in which any shortcoming could result in serious reputational damage and heavy fines for companies or individuals.

Every day, Arendt works to ensure that its clients remain compliant with their AML/CFT requirements in this constantly changing environment, so as not to become unknowing contributors to illicit activity. Arendt is uniquely positioned to understand and help you face the many challenges entailed by your AML/CFT obligations. We would be pleased to assist you in the prevention and detection of ML/TF concerns and risks while also equipping your company to properly respond to any deficiencies, and to implement a suitable AML/CFT compliance programme where necessary.

Your key contact:
Sandrine Périot, Partner Arendt Regulatory & Consulting
sandrine.periot@arendt.com
T +352 40 78 78 8080

About Arendt's Forensic Investigations, Corporate Intelligence & Litigation Support practice

The team comprises forensic investigators and analysts, encompassing a broad range of expertise and technologies to help clients respond efficiently to regulatory investigations by various authorities covering a wide area of issues: money laundering, corruption, sanctions breach, greenwashing, accounting fraud, market abuse and other financial crime. In internal investigations (such as fraud, misconduct, harassment or whistleblowing), we find the facts that matter and deliver actionable intelligence in an objective and independent manner.

Investigations can vary widely: they can change suddenly in scope and are often time-critical. They require decisive and immediate action and support from experts: data needs to be collected, preserved and analysed, and key witnesses or suspects identified and interviewed, all while business continues as usual.

Forensic technology plays a crucial role in investigations involving electronic evidence. We assist clients in managing vast amounts of data and navigating the business and legal processes efficiently. Using state-of-the-art software and infrastructure (with Relativity, our e-Discovery and document review solution), we offer a range of services including data collection, evidence assessment and document review, which combine with our data analytics experts to enable our clients to respond effectively to legal or regulatory incidents and crises.

We ensure that investigations are compliant with local and global data protection and privacy regulations, working alongside our data protection legal specialists.

We help you to assess, prevent, detect and respond to pressure and risks:

- Internal & Regulatory Investigations
- Forensic Technology (Relativity in-house tool, data analytics and mobile forensic)
- Corporate Intelligence
- Compliance & Ethics
- Disputes & Litigation Support

Your key contact:
Stéphanie Lhomme, Head of Forensic Investigations,
Corporate Intelligence & Litigation Support practice
stephanie.lhomme@arendt.com
T +352 40 78 78 7774

Ready to discuss your level of preparedness?

Need immediate assistance for a dawn raid?

About Arendt

your legal, tax and business services firm in Luxembourg

Arendt combines the entire value chain of services dedicated to Asset Managers, Banks, Insurers, Public Institutions, Commercial Companies and Private Clients operating in Luxembourg.

Legal & Tax

We assist clients in structuring and running their business from a legal and tax standpoint across Luxembourg. Our teams directly serve international clients or work in close collaboration with foreign partner law firms.

Together, with our regulatory consultants and investor services experts, we bridge the gap between legal/tax advice and its implementation. We deliver best-in-class services for our clients' business life cycle.

With over 450 legal experts at Arendt & Medernach, we are able to advise you in the following areas:

Administrative Law, Property, Construction & Environment	Banking & Financial Services	Business Crime	Commercial & Insolvency	Corporate Law, Mergers & Acquisitions
Litigation & Dispute Resolution	Employment Law, Pensions & Benefits	EU Financial & Competition Law	Finance & Capital Markets	IP, Communication & Technology
Insurance & Reinsurance Law	Investment Management	Private Clients	Private Equity & Real Estate	Tax Law

Arendt & Medernach S.A
Registered with the Luxembourg bar
RCS Luxembourg B 186371

arendt.com

41A avenue JF Kennedy
L-2082 Luxembourg
T +352 40 78 78 1

06/2024