



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

Luxembourg Investment Fund (Manager) !

Operating Procedure “Inspections and Dawn Raids”

This template is designed to help you create an operating procedure that will guide you in preparing for and handling inspections or dawn raids in a professional manner. The purpose of the inspection process is to ensure that employees act as intended by the responsible persons in such cases.

Reference:

- Code of Criminal Procedure (Code d’instruction criminelle, CIC)
- Fiscal Code (Abgabenordnung, AO, „Loi générale des impôts“)
- Law of 5 April 1993 on the Financial Sector
- Data Protection Law (Loi du 1er août 2018 portant organisation de la CNPD)
- Labour Code (Code du travail)
- Competition Law

In practice, a specific legal basis is almost always required; judicial warrants are usually mandatory, especially in criminal and competition law matters.

Version: 17 July 2025

This document may be revised and reissued as its content evolves over time.

License: Luxembourg Investment Fund (Manager) ! Operating Procedure “Inspections and Dawn Raids”, <https://financialcrime.lu/templates/index.html> © 2025 by [concilio et labore GmbH](#) is licensed under [CC BY-SA 4.0](#)



This license requires that reusers give credit to the creator. It allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, even for commercial purposes. If others remix, adapt, or build upon the material, they must license the modified material under identical terms.

Disclaimer: We make no representation or warranty of any kind, express or implied, regarding the accuracy, adequacy, validity, reliability, availability, currentness or completeness of the information contained in this document.



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

Contents

1. Document History	3
2. Amendments.....	3
3. Terms.....	4
4. Process	6
4.1 Before the Inspection.....	6
4.1.1 Training & awareness-raising	6
4.1.2 Legal assistance for employees.....	7
4.1.3 Dealing with cloud services and international data access.....	8
4.2 During the Inspection.....	9
4.2.1 Preparations	10
4.2.2 Immediate first steps.....	11
4.2.3 Dealing with Search Warrants.....	12
4.2.4 Shadowing (accompanying the authorities)	12
4.2.5 Involvement in Inspection.....	14
4.2.6 Dealing with interrogations	15
4.2.7 Handling confidential / privileged documents	16
4.2.8 Dealing with private devices (Bring Your Own Device)	16
4.2.9 Dealing with large amounts of data & splitting data.....	17
4.2.10 Sealing of rooms.....	18
4.2.11 Internal meeting.....	19
4.2.12 Final Meeting with Inspector.....	19
4.3 After the Inspection.....	20
4.3.1 Follow-up & communication.....	20
5. Escalation.....	21
5.1 Escalation levels & coordination	21
Annex 1 Information mail to employees in case of an Inspection.....	22
Annex 2 Checklist “Golden Rules”	23



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

1. Document History

Release Date	Description	amended by	reviewed by

2. Amendments

This Operating Procedure must be reviewed regularly, at least annually, by the responsible employee and amended if necessary. Affected employees must be notified of any amendments to this Operating Procedure and the processes described.



3. Terms

The following indicative definitions, which do not override equivalent definitions in national law, have been developed only for the purposes of this Operating Procedure.

Inspection (or Dawn Raid)	An Inspection or Dawn Raid refers to an unannounced visit by an authority – regardless of its type – conducted at the premises of the Entity or any other location involving employees of the Entity, with the purpose of reviewing information related to or owned by the Entity.
Inspector(s)	The individual(s) authorized to carry out the Inspection.
On-Site Visit	An On-Site Visit, is not an unexpected inspection but occurs after prior notice has been given. Nevertheless, the obligations described in this process must be observed in the same way.
Privilege	Communications between a lawyer and their client are inherently subject to legal professional privilege and are therefore confidential. ¹
Search Warrant / Authorization Notice	A document presented by the Inspector(s) to demonstrate their authority to perform the inspection, specify the company being inspected, and state the purpose of the Inspection.

¹ From a data protection perspective, under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals regarding the processing of personal data and the free movement of such data, which repealed Directive 95/46/EC (“the Data Protection Regulation”), the controller is permitted to process (i.e., disclose) personal data if such processing is necessary to comply with a legal obligation to which the controller is subject (Article 6(1)(c) of the Data Protection Regulation). Although the data subject generally has the right to object and to restrict processing, these rights do not apply where processing is based on a legal obligation. In this context, this means that data subjects cannot prevent the mandatory disclosure of their personal data.

On the other hand, Article 35 of the Law on the Lawyer's Profession of 10 August 1991 states that professional secrecy between a lawyer and client is absolute and that collecting documents covered by this privilege is never permitted. In practice, however, documents protected by professional secrecy may be seized during inspections because they are often taken together with other materials. In such cases, it is possible to challenge the seizure by filing a complaint.



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

Shadower

A person assigned to accompany the Inspector(s), document their actions, and report on activities performed by the Inspector(s).



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

4. Process

The process outlines the actions to be taken if an Inspection occurs and includes a checklist that should be kept readily accessible near the entrance of the Entity's office.

An Inspection can be broken down into three phases:

- before the Inspection;
- during the Inspection;
- after the Inspection has concluded.

4.1 Before the Inspection

This process begins the moment an Entity employee becomes aware that an Inspection will take place. In most cases, this awareness arises when the Inspector arrives and introduces themselves after ringing the doorbell at the office entrance. The employee receiving the Inspector is then responsible for promptly notifying the designated contact person or the relevant department within the Entity, in accordance with internal procedures.

From this initial notification, all steps outlined in the Inspection process must be followed without delay. This includes retrieving the checklist near the entrance, alerting management, and ensuring all necessary measures are in place to comply with the Inspection requirements. The process is designed to ensure the Entity responds swiftly and appropriately from the moment an Inspection is announced.

4.1.1 Training & awareness-raising

Comprehensive training and awareness-raising for employees is an essential prerequisite for acting professionally and in accordance with the rules in the event of an Inspection. Only if everyone involved knows the procedures, rights and obligations can mistakes be avoided and risks for the Entity and employees minimized.

As part of the preparation, specific training should be carried out regularly for selected groups of employees. These include, in particular, reception staff, IT teams, compliance officers, the legal department and managers in relevant areas. These training courses provide practical knowledge on how to behave when authorities visit, how to handle sensitive information and how to comply with data protection and compliance regulations.

A central component of the training is the communication of rules of conduct, such as keeping calm, not providing unauthorized information, not handing over documents without consent and



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

informing the responsible contact persons immediately. It is equally important to explain rights such as the right to remain silent and the importance of legal assistance during questioning.

In addition, awareness-raising should also address technical aspects, such as how to handle IT systems during an Inspection, how to stop automatic data deletion processes and how to ensure documentation obligations are met.

Regular repetition of the training courses and the provision of easily accessible information materials, checklists and instructions are recommended to ensure that this knowledge is firmly anchored. This means that employees can quickly access the knowledge even in stressful situations.

Targeted training measures not only increase employees' confidence, but also raise awareness of the importance of compliance and legal precautions. This strengthens the entire organization and makes a significant contribution to managing Inspections professionally and reducing corporate risks.

4.1.2 Legal assistance for employees

A key aspect of dealing with Inspections is ensuring that affected employees have appropriate legal assistance. As interrogations are often associated with considerable legal and personal risks, it is essential that employees have the opportunity to be accompanied and advised by a qualified criminal defense lawyer at all times.

The Entity ensures that independent and experienced external legal counsel is available for all employees who are questioned or accused as part of an Inspection. It is important that this legal counsel exclusively represents the interests of the employee and acts independently of the Entity. The separation of interests between the Entity and individual employees is fundamental in order to avoid conflicts of interest and ensure an effective defense.

In practice, this means that external defense lawyers are always involved in addition to the Entity's internal legal advisors or compliance officers. These external lawyers have the necessary specialist expertise in criminal and white-collar criminal law and can provide individual and comprehensive support to the employees concerned.

The Entity communicates early and transparently about the offer of such legal advice. Employees are encouraged to accept this offer, particularly in view of the fact that statements made without legal advice can lead to unwanted self-incrimination. However, it is respected if employees wish to choose their own lawyer who is independent of the Entity.



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

In addition, the Entity ensures that a list of qualified defense attorneys who can be contacted quickly is kept available in preparation for possible Inspections. This ensures that interrogation situations are handled swiftly and smoothly.

Depending on internal regulations, the costs for legal assistance can be borne by the Entity, especially if there is a close connection to the professional activity. However, it should be clearly regulated in advance under which conditions and to what extent costs will be covered.

4.1.3 Dealing with cloud services and international data access

In today's digital world, company data is frequently stored in cloud services that are often located on servers in different countries. This relocation of data to international data centers poses particular challenges in the context of Inspections, especially with regard to the access rights of investigating authorities and compliance with legal requirements.

In principle, cloud data is subject to the law of the country in which the servers are located. Luxembourg investigating authorities therefore do not have unrestricted sovereign rights to foreign cloud servers. In order to gain access to such data, they usually have to cooperate with the competent authorities in the respective country via formal requests for mutual legal assistance. This process can be time-consuming and complex.

Excursus: E-Evidence Regulation

From August 18, 2026, after a three-year transition period, the so-called E-Evidence Regulation ([Regulation \(EU\) 2023/1543](#)) will come into force, which will provide law enforcement authorities within the European Union with simplified options for accessing digital evidence, including cloud data. This includes both freeze orders and production orders. Companies must prepare for these changes and adapt their internal processes accordingly.

When dealing with cloud services, it is advisable not to grant careless or spontaneous access to foreign cloud data. Instead, any release or backup of data should always be carried out in close consultation with legal counsel. This way, it is possible to check which data is actually relevant and minimize risks relating to data protection, trade secrets and international legislation.

In addition, it makes sense to create an overview of the cloud services used and their locations in advance and to check contractual regulations with the providers. This makes it easier to respond in a structured and legally compliant manner in the event of an Inspection.



Overall, dealing with cloud services and international data access requires careful legal and technical preparation. Only a coordinated approach between senior management, the IT department and legal counsel can ensure that investigating authorities are granted appropriate access while at the same time safeguarding the interests of the Entity and the applicable data protection regulations.

4.2 During the Inspection

During an Inspection, the Inspector's main focus is often the Entity's IT environment. They may attempt to connect to the Entity's IT systems using their own equipment, such as laptops, external hard drives, or other electronic devices, to access, review, or copy digital data. IT staff must be present to monitor this access, ensure compliance with security protocols, and document all IT system activities.

However, the scope of an Inspection is generally much broader and may include a comprehensive review of physical and digital assets. Inspectors may examine and search the following areas and items:

- **Buildings and premises:**
Any property owned, leased, or otherwise used by the Entity – including offices, meeting rooms, storage areas, and common spaces – may be inspected. Inspectors may walk through these areas to look for documents, materials, or evidence relevant to their investigation.
- **Desks, cabinets, and file archives:**
The workspaces of employees, including their desks, drawers, filing cabinets, and physical archives, may be searched for physical documents or other materials considered relevant.
- **Business documents and records:**
Inspectors may request access to all types of business documentation. This includes, but is not limited to, internal and external correspondence (e.g., letters, emails, faxes).
- **Personal items and electronic devices:**
Briefcases, laptops, address books, smartphones, USB drives, and other portable devices found on the premises may be reviewed if there is reasonable suspicion that they contain relevant company information.
- **Data stored on servers and other IT infrastructure:**
Inspectors may request access to the Entity's servers, databases, backup systems, and cloud storage. As part of their investigation, they may search for, review, or extract digital data.
- **Individuals present on site:**
Inspectors may question employees or visitors present during the Inspection. This could involve interviews or requests for explanations regarding certain documents or procedures.



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

➤ **Company vehicles:**

Cars owned or operated by the Entity may also be subject to inspection. Inspectors may search these vehicles for documents or electronic devices that could contain relevant information.

Given the broad scope of the inspection, it is important for all staff to be aware that it may not be limited to electronic data or IT systems. Any location, item, or person connected to the Entity could be involved in the Inspection process. Employees should cooperate fully and ensure that all actions taken by Inspectors are properly documented by the assigned Shadowers. In cases involving access to sensitive or privileged materials, such as communications covered by legal Privilege, immediate legal advice should be sought.

4.2.1 Preparations

As soon as it becomes clear that an Inspection will take place, a **support team** should be assembled to ensure that the process is managed efficiently and in accordance with all internal protocols and regulatory requirements. The support team should be composed of staff members from different key areas, including:

➤ **Administrative support:**

Responsible for coordinating logistical aspects, handling documentation, and assisting with communication between the Inspectors and the relevant personnel within the Entity.

➤ **IT support:**

Staff familiar with the Entity's IT infrastructure, systems, and data storage practices. Their role is to provide technical assistance to the Inspectors as needed, ensure secure access to electronic records, and address any IT-related questions or issues that may arise during the Inspection.

➤ **Shadower:**

Assign at least one Shadower for each Inspector present. The Shadower's task is to accompany the Inspector throughout the entire Inspection, observe all activities, and take detailed notes on all actions, requests, and comments made by the Inspector.

In addition to the support team, it is advisable to set up a **response team** to address all significant issues that may need immediate or high-level attention during the Inspection. The response team should include at minimum:

➤ **Members of the management board:**

To provide strategic oversight, make critical decisions on behalf of the Entity, and coordinate with Inspectors if required.



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

➤ **Legal representatives:**

To give immediate legal advice, handle interactions regarding professional privilege or confidentiality concerns, and participate in shadowing if necessary.

Before the Inspection commences or immediately upon its start, it is essential to inform all employees about the situation. This can be done either verbally or by distributing a pre-written email (template provided in Annex 1). Employees should be reminded of their obligations during an Inspection and instructed to cooperate fully while referring any questions or requests from Inspectors to the designated contacts.

Furthermore, it is crucial to take technical precautions by immediately suspending any automatic processes that may result in the deletion or alteration of data. This includes stopping scheduled data protection deletion routines or any other automated processes that could impact the availability or integrity of records relevant to the Inspection.

4.2.2 Immediate first steps

Make every reasonable effort to promptly carry out the following steps:

- Remain calm and courteous when receiving the Inspector.
- Retrieve the checklist located near the entrance of the office.
- Cooperate fully with the Inspectors and comply with all Inspection requirements.
- Allow the Inspectors to enter the premises and, if possible, guide them to the large meeting room.
 - If the Inspector insists, permit them to use an office room and take control of all means of communication.
- Verify the identity and authorizations of the Inspectors. If permitted, make copies of all relevant documents. If making copies is not allowed, write down all pertinent details, including:
 - Names,
 - Job titles,
 - The agency or regulatory body they represent,
 - Contact information,
 - The stated purpose of their visit as listed on the authorization notice.
- Inform the responsible employees and seek legal assistance immediately (refer to chapter 4: Responsible employees/contacts).
- Request that the Inspectors allow time for legal counsel and responsible employees to arrive.
 - Ask for permission to notify the group's legal department, if applicable.



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

4.2.3 Dealing with Search Warrants

A central component of every inspection or search is the Search Warrant, which forms the legal basis for entering business premises and seizing evidence. The correct handling of this document is essential in order to verify the legality of the measure and to protect the rights of the Entity and its employees.

As soon as investigating authorities appear on site, insist immediately that the search warrant is presented. This must clearly legitimize the searching authority and specify the places to be searched as well as the scope and purpose of the Inspection. It is important to examine the warrant carefully, ideally together with the legal counsel present, in order to identify ambiguities or unauthorized measures at an early stage.

In accordance with the legal requirements, a copy of the Search Warrant must be handed over to those responsible at the Entity - usually at the beginning of the search or at the latest at the end of the measure. If this is not done immediately, it must be insisted upon. In exceptional cases, an oral Search Warrant may also be issued; in such cases, a written Search Warrant must be submitted immediately.

The Entity documents receipt of the decision, makes a copy if necessary and forwards it to the legal counsel without delay. This documentation serves as the basis for the subsequent legal review and possible legal remedies.

During the Inspection, the scope of the search objects and areas specified in the Search Warrant should be continuously compared with the actual actions of the authorities. If measures outside the authorized scope are carried out, this must be recorded immediately and, if necessary, addressed by the legal counsel.

The Search Warrant also forms the basis for determining which documents or data may be seized or confiscated. Particular attention must be paid to the exact wording in the Search Warrant in order to prevent the unlawful seizure of documents.

4.2.4 Shadowing (accompanying the authorities)

During an Inspection, it is very important that the Entity continuously accompanies the investigating authorities and carefully monitors their activities - this process is known as "shadowing". The aim of shadowing is to ensure compliance with the legal framework, guarantee the protection of sensitive information and enable complete documentation of the process.

For this task, (ideally specially trained) employees ("Shadowers") are appointed to accompany the Inspectors every step of the way, observing and recording their actions. Shadowers are



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

responsible for controlling the Inspectors' access to sensitive areas and ensuring that only the rooms and documents permitted in the Search Warrant are viewed or taken away.

During the escort, Shadowers take detailed notes, including questions asked, documents viewed and data collected. They also document which physical or electronic items were copied or seized. It is important that Shadowers pay particular attention to the protection of privileged documents, such as correspondence between attorneys and clients or internal defense documents. Such documents may only be shown or copied after consultation with legal counsel.

Shadowers make two additional copies for all physical documents collected: one remains with the Entity and another is given to legal counsel. Electronic copies are also backed up and checked. This extensive documentation forms the basis for a later legal assessment and possible appeals.

In addition, Shadowers have the right to inform legal counsel immediately in the event of discrepancies or suspected violations of the Search Warrant. They therefore act as an important interface between the investigating authorities and senior management.

Shadowers are selected carefully; they should have a good understanding of company structures and the legal framework and be able to act professionally and calmly even in stressful situations.

In Summary, Shadowers have the following responsibilities:

- **Maintain a comprehensive record of the Inspection:**
Document all questions posed by the Inspector and the responses provided by employees. This creates a clear account of the topics covered and the information disclosed during the Inspection.
- **Monitor document searches:**
Note the search terms and keywords used by the Inspectors when reviewing files. Record which files, folders, or databases were accessed and which specific documents or categories of information were requested or examined.
- **Track reviewed and collected documents:**
Keep a detailed list of all documents that have been viewed by the Inspector, as well as those that have been physically collected or copied during the Inspection.
- **Copying of electronic documents:**
Whenever an Inspector copies electronic files or data, ensure that copies are also made for the Entity's own records.
- **Copying of physical documents:**
For any paper documents collected by the Inspector, make two additional copies: one set to remain with the Entity's records and another set to be provided to legal counsel for review and future reference.
- **Privilege and relevance check:**



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

Examine each document prior to its collection or disclosure to determine whether it is protected by legal privilege or contains sensitive business information. Only disclose such materials in accordance with legal advice.

➤ **Control over materials taken by Inspectors:**

- Original documents should generally not be removed from the premises by Inspectors.
- Inspectors may, however, make copies of documents and take these copies with them.
- Documents containing trade or business secrets must be clearly marked as such before any copies are provided to Inspectors.
- If a document is incomplete, explain this fact to the Inspector and arrange for missing information to be provided as soon as possible.

4.2.5 Involvement in Inspection

Participating in an Inspection can be challenging, and the role of a Shadower requires particular care and attention. Not everyone is suited to serve as a Shadower, as it demands a high level of responsibility, vigilance, and composure.

Anyone who interacts with Inspectors during the Inspection should keep the following recommendations in mind:

➤ **▶ Do not incriminate yourself:**

Avoid making statements or providing information that could be self-incriminating or that could potentially expose the Entity or its employees to liability.

➤ **▶ Do not volunteer documents unless specifically requested:**

Only provide documents that are directly and explicitly requested by the Inspector. Do not offer additional materials or information beyond what has been asked for.

➤ **▶ Do not speculate or elaborate unnecessarily:**

Limit your answers to the information requested. Do not guess, hypothesize, or provide details beyond the scope of the question posed.

➤ **✔ Respond to specific questions directly:**

If the Inspector asks a clear, specific question, it can be answered on the spot with straightforward information.

➤ **✔ Keep answers and notes factual and neutral:**

All responses and written notes should be strictly factual, objective, and free from personal opinions or emotional language. Avoid any statements that leave room for interpretation or subjective assessment.

➤ **✔ Consult a lawyer before addressing broader questions:**



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

If the Inspector asks wide-ranging or complex questions, wait for legal counsel before providing an answer. This ensures that responses are legally sound and that sensitive or privileged information is protected.

4.2.6 Dealing with interrogations

During an Inspection, investigating authorities may question employees or Entity representatives about certain facts. Dealing with such interrogations requires special attention in order to protect the rights of the persons concerned and to support the Entity in the best possible way.

As a general rule, employees should not make any substantive statements on the matter before qualified legal counsel is present. This applies both to persons against whom suspicion is directed (the accused) and to witnesses. It is important not to volunteer information that goes beyond the specific questions or contains speculation. Answers should always be factual, concise and limited to the essentials. In order to avoid self-incrimination, employees have the right to refuse to give evidence, especially if it is unclear whether giving evidence could be detrimental. In addition, informal discussions with Inspectors should be avoided, as even casual comments can be interpreted as incriminating.

Every employee has the right to have their own lawyer present during questioning. The Entity ensures that affected employees are provided with an independent external defense lawyer if required, who exclusively represents their interests. It is very important to avoid conflicts of interest between Entity and employee representatives. Employees should be fully informed about their rights and obligations before a hearing begins.

The Entity assumes a coordinating role by providing expert support for the hearing and managing communication with the investigating authorities. The legal department or a designated coordinator ensures that the hearings are conducted in an orderly manner and supports employees in safeguarding their rights. At the same time, the Entity expressly points out that no undue influence or pressure may be exerted on employees. In particular, it is prohibited to urge employees not to testify or to make certain statements.

Wherever possible, questioning should not take place immediately during the Inspection on site, but in a separate, protected setting at a later date. This allows for better preparation as well as structured and coordinated conduct in consultation with the respective legal counsel. The dates for hearings should be announced well in advance to give the parties involved sufficient time to prepare.



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

4.2.7 Handling confidential / privileged documents

The protection of confidential and privileged documents is of particular importance in the context of Inspections. Such documents are often protected by legal requirements or professional confidentiality obligations and may not be inspected, copied or seized without the express consent of legal counsel.

Confidential documents include correspondence between the Entity and external lawyers, internal defense documents, strategic plans and documents containing trade secrets or personal data. Privileged documents are in particular those that are subject to attorney-client Privilege and therefore enjoy a particularly high level of protection.

Employees who come into contact with such documents in the course of an Inspection must be trained to recognize them and restrict access. Consultation with legal counsel is always required prior to inspection by investigating authorities. If necessary, the relevant documents should only be shown after they have been checked and approved by the lawyer.

The investigating authorities are generally not permitted to copy or take privileged documents. Should an Inspector nevertheless wish to make copies, this must be actively prevented and appropriate objections must be raised. In some cases, it may be necessary to view only selected excerpts of a document in order to document the privileged status without disclosing the entire content.

To ensure the integrity of these documents, it is advisable to ensure that they are handled separately during the search - for example, by sealing them or storing them separately. Shadowers play an important role here by monitoring the protection of privileged documents and ensuring that they are not used without authorization.

If in doubt about the status of a document, legal counsel should always be consulted to avoid unintentional disclosure or breach of professional confidentiality.

By taking a consistent approach to handling confidential and privileged documents, the Entity protects its legal interests and maintains the confidentiality of sensitive information even in critical situations such as Inspections.

4.2.8 Dealing with private devices (Bring Your Own Device)

In modern companies, it is increasingly common for employees to use private devices such as smartphones, tablets or laptops for business purposes - a concept known as "Bring Your Own Device" (BYOD). This trend poses particular challenges when it comes to Inspections by investigating authorities, as private and professional data may be stored on the same device.



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

When dealing with private devices, it should first be noted that they can be subject to searches and seizures in the same way as company-owned devices if there is suspicion against the user and the legal requirements are met. However, there is a particularly high level of privacy protection for private devices, as they often contain personal and non-work-related data.

The Entity informs employees at an early stage and in detail about their rights and obligations in the event of searches of private devices and recommends storing sensitive private data separately from work-related information wherever possible. In addition, clear internal guidelines should be in place that regulate the handling of private devices and ensure the protection of personal data.

In the event of a search, particular care must be taken to ensure that investigating authorities only access the data relevant to the proceedings. As private devices often contain large amounts of personal data, the accompaniment of the search by experienced legal advisors and IT specialists is crucial in order to protect the privacy of employees and prevent the unnecessary disclosure of private information.

Special legal frameworks apply when unlocking private devices. While employees are obliged to hand over passwords or access data for company-owned devices, this is more limited for private devices. Biometric unlocking methods such as fingerprint or facial recognition are often regarded by the authorities as permissible toleration, while the issuing of passwords cannot usually be enforced. Employees should therefore be informed about these differences.

The Entity supports affected employees in acting calmly and prudently in such situations and ensures that legal counsel is involved at an early stage. At the same time, it is recommended to promote technical measures such as the use of separate work profiles on private devices in order to keep business and private data strictly separate.

4.2.9 Dealing with large amounts of data & splitting data

Modern inspections and searches, especially in the IT sector, often lead to the seizure of enormous amounts of data. This includes emails, digital documents, chat histories and other electronic information that may be relevant to investigations. Handling such large amounts of data requires careful planning and structuring to ensure both the protection of sensitive information and efficient processing.

A key step is to work together with the investigating authorities and internal IT and legal experts to make a clear distinction between data that is relevant to the proceedings and data that is not. To this end, the secured data is systematically reviewed and divided into relevant “data areas”. This division allows only the information that is actually important for the Inspection to



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

be included in the investigation file, while irrelevant or particularly sensitive data remains separate.

This approach offers several advantages: Firstly, it ensures the protection of business secrets, personal data and other sensitive content. Secondly, it helps to speed up the investigation process, as the authorities can access a clearly structured and filtered set of data. In addition, the separation of data facilitates the subsequent return of irrelevant data carriers or files to the Entity.

It is advisable to coordinate this process of data preparation transparently with the Inspectors and to have it accompanied by experienced lawyers. This ensures that the criteria for separating the data are comprehensible and accepted by all parties. Such cooperation promotes trust between the Entity and the investigating authorities and can make the process more efficient overall.

In addition, the Entity should ensure that the technical means for data analysis and separation are available and that employees are trained accordingly. If necessary, external expertise can also be brought in to carry out the data preparation.

Overall, the deliberate and structured handling of large volumes of data is a key factor in successfully dealing with Inspections. It enables the Entity to protect its interests, meet compliance requirements and at the same time offer the investigating authorities orderly cooperation.

4.2.10 Sealing of rooms

Some Inspections may last for several days, and during this time Inspectors may gather documents to review at a later stage. In certain cases, the Inspector may decide to seal off a room in order to secure and store collected documents separately from other materials. Even if the Inspector is not able to physically seal the room themselves, entry to this area must be strictly prohibited.

Simply locking the door is not sufficient. Access restrictions should be clearly communicated by placing a prominent warning sign on the door, and, if necessary, by assigning security personnel to monitor the area. It is essential to ensure that all staff members – including cleaning and security personnel – are informed about the sealed room and understand that entry is strictly forbidden until the restriction is lifted by the Inspector or other authorized person. This helps maintain the integrity of the Inspection process and prevents any unauthorized handling or removal of secured documents.



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

4.2.11 Internal meeting

The employees involved into the Inspection should be brought together for an internal meeting, attended by the legal counsel, at the end of each day.

At the end of each day during the Inspection, employees involved in the process should gather for an internal meeting, which should also be attended by the legal counsel.

During these meetings, the following actions must be taken:

- **Consolidate all notes:**
Collect and review notes from all staff members involved to ensure a complete and accurate record of the day's events.
- **Ensure notes remain factual:**
Check that all entries are objective, precise, and free from opinions or speculation.
- **Clarify next steps for staff:**
Make sure every employee understands their responsibilities and how to proceed on the following day of the Inspection.
- **Reinforce restricted access:**
Remind all participants, including cleaning and security staff, that no one is permitted to enter any sealed rooms.
- **Prepare communications if needed:**
If appropriate, work with legal counsel to draft a press release or prepare responses to potential external inquiries.

4.2.12 Final Meeting with Inspector

As the Inspection is nearing completion, request a final meeting with the Inspectors to address the following points:

- **Prepare an inventory of all documents copied:**
Ask the Inspectors to provide a detailed list of every document that has been copied during the Inspection.
- **Cross-check the inventory with your own records:**
Carefully compare the Inspector's inventory with the notes and records maintained by the Shadows to ensure accuracy and consistency.
- **Confirm that all copied documents are recorded:**
Verify that every document which has been copied or taken by the Inspectors is properly listed in both the Inspector's and your own inventories, so that nothing is missing or unaccounted for.



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

4.3 After the Inspection

The Inspection is considered concluded once the Inspectors have left the premises and it has been confirmed that they do not intend to return. Only at this point should post-Inspection procedures begin.

4.3.1 Follow-up & communication

Once the Inspection has been completed, a crucial phase begins: systematic follow-up and careful management of internal and external communication. This step is decisive for how the Entity deals with the effects of the measure and what consequences result from it.

Immediately after the investigating authorities have left, an internal meeting should be held with all employees involved and the legal counsel. The information collected, the recorded procedures and the documents seized are jointly evaluated and checked for completeness and legality. The aim is to obtain a comprehensive picture of the facts and to record any discrepancies or infringements on the part of the authorities.

The Entity obliges all employees involved to maintain confidentiality about the course of the Inspection in order to protect internal information and avoid further damage. At the same time, the management informs relevant bodies such as the Supervisory Board, Board of Directors or, if applicable, shareholders promptly about the situation and the current status.

External communication should be strategically planned and coordinated. Particularly in the case of listed companies or in regulated sectors, it should be checked whether and to what extent a report to supervisory authorities (e.g. CSSF) or other supervisory bodies is required. It is also important to consider how to respond to business partners, customers and the public in order to maintain trust and minimize reputational risks.

Employment law issues must also be clarified as part of the follow-up. Depending on the nature of the allegation, it may be necessary to consider measures against the employees concerned, such as leave of absence or dismissal, in order to protect the Entity and maintain compliance.

In addition, the Entity should promptly carry out a comprehensive review of the facts - internally or with the support of external consultants. This enables sound preparation for possible further investigations or proceedings as well as the targeted development of countermeasures.

A clear line of communication is essential here: responsibilities for internal and external communication must be defined in order to avoid contradictory or uncontrolled statements. Ideally, a central contact person should be appointed to act as an interface between the internal teams, legal counsel and external stakeholders.



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

5. Escalation

5.1 Escalation levels & coordination

A clearly defined escalation and coordination process is crucial in order to be able to react quickly and effectively in the event of an Inspection. Structured processes ensure that all relevant decision-makers and specialist departments are involved at an early stage and that the measures are managed centrally.

The first point of contact when an Inspection becomes known is usually the employee directly affected. They immediately inform a designated contact person or an internal coordination team that has been specially trained to deal with such situations. This team ideally consists of members of the legal department, compliance, IT and senior management.

The next step is to notify and involve the management board. The management board bears overall responsibility for the procedure and ensures that all necessary resources are made available. At the same time, internal and external communication is coordinated to ensure a uniform approach.

The Board of Directors of the management company is also informed, particularly if the situation is more complex or has a significant impact on the Entity. In the case of fund management companies, the Board(s) of Directors of the respective fund(s) should also be involved, insofar as it is/they are affected and legally permissible, in order to ensure transparency and control there as well.

In parallel to the internal escalation, the involvement of external consultants - in particular specialized lawyers and IT experts - is organized. They provide support with the legal review, monitoring of the search and technical handling, particularly in the case of IT searches.

Coordination also includes setting up a central contact person or a crisis team to act as a link between all parties involved. This contact person ensures the prompt forwarding of information, the documentation of all processes and coordination with authorities and external service providers.

The escalation stages are as follows:

Staff

⇒ Management Board



⇒ Board of Directors

Response Team

Support Team



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>









Annex 1 | Information mail to employees in case of an Inspection

Dear all,

An inspection of our office by *[insert name of inspecting authority]* will take place today.

As a company, we will fully cooperate with the inspector(s), and every employee is obligated to do the same.

Therefore, please follow these rules:

-  Keep calm and be friendly.
-  Answer the questions you are asked.
-  Consult a lawyer before addressing broader questions.
-  Take notes on everything you are involved in during the inspection.
-  Do not destroy any documents.
-  Do not say more than is asked of you.
-  Do not speculate or elaborate unnecessarily.
-  Do not communicate with anyone about the inspection.

After the inspection, we will have a meeting with all of you to discuss the results.

Kind regards,

[insert name]



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>

Annex 2 | Checklist “Golden Rules”

Inspection and Dawn Raid Golden Rules

Proceed as follows:

- Verify the identity of the Inspectors.
- Clarify the extent of their powers and the boundaries of the Inspection.
- Document all events that take place.
- Provide the Inspectors with a secure room and access to a photocopier.
- Make sure Inspectors are never left alone without supervision (‘Shadowing’).
- Stop any destruction of documents or information.
- Make efforts to stop inspectors from viewing documents protected by legal privilege.
- Try to stop inspectors from making inquiries beyond their official authority.
- Postpone resolving any disputes to a later time.

OK You may call the following persons to request assistance.

You do **not** need to consult senior management prior to this step.



Law Firm ABC

John Doe, Ph.D.

Partner

john.doe@lawfirmabc.com

T +352 98 76 54 321



Law Firm ABC

Jane Doe, LL.M.

Partner

jane.doe@lawfirmabc.com

T +352 98 76 54 320

M +352 621 98 76 5



FinancialCrime.lu

Combating Financial Crime

Join the Fight - Empowering Justice, Protecting Finances.

<https://financialcrime.lu>