

AFM Integrity Policy

In short An unimpeachable reputation is essential for the AFM. Acting with integrity is thus paramount. The AFM Code of Conduct helps as an integrity compass for your day-to-day work. The AFM Integrity Policy is a supplement to the Code of Conduct. The Regulations in this policy describe the ways in which the AFM handles matters such as private investment, screening and the integrity screening of employees, the reporting of apparent or suspected wrongdoings, integrity violations and undesirable behaviour, sanctions and how the AFM deals with complaints about undesirable behaviour. These arrangements have been put in place so that we, as an organisation, act with integrity and continue to do so.

Table of contents

1. The regulation on private investments	2
2. The screening	8
3. The regulation on reporting apparent or suspected wrongdoings, violations of integrity and undesirable behaviour	21
4. The regulation on integrity investigations	33
5. The regulation on sanctions	38
6. The regulation on complaints of undesirable behaviour	43

1. The regulation on private investments

1.1 Introduction

Insider trading, or the appearance thereof, interferes with the fair and efficient operation of financial markets, and has the potential to greatly damage the integrity and reputation of the Dutch Authority for the Financial Markets (AFM) and its employees. While AFM employees are allowed to make private investments, they are, however, subject to conditions and restrictions that are aimed at preventing insider trading or the appearance of insider trading. That information is set out in this Regulation.

By virtue of this Regulation, the AFM seeks maximum alignment with the prohibition on insider trading set out in EU Regulation no. 596/2104 (the Market Abuse Regulation or MAR). In addition to this Regulation, there is a closed list and insider files may be applicable. See the 'Work instructions for updating the closed list' and the 'Explanatory notes to insider files' at Connect.

In case of any doubt or ambiguity, please always contact the compliance officer.

What is inside information?

Inside information is having information that:

- is not publicly available,
- that is specific, and
- that directly or indirectly relates to one or more issuers or one or more financial instruments, such as shares or bonds, and
- which, if made public, could have a significant impact on the price of those financial instruments and/or the price of related derivative financial instruments.

This could include information related to companies subject to supervision (such as changes to a board) and their customers (such as issues or takeovers). The same applies to non-public information obtained from other supervisory authorities.

Acting in violation of these Regulations can be deemed a serious breach of the trust that the AFM must be able to have in its employees, and on that basis can lead to one or more appropriate sanctions. See the Regulation on sanctions.

1.2 Who does the regulation apply to?

This Regulation applies to all AFM employees as defined in the Regulation on private investment as well as all former employees up to two months after leaving the employment of the AFM. Further rules for members of the Executive Board and the Supervisory Board are included in Paragraph 6. The compliance officer may make an exception to this Regulation for employees or prospective employees who work or will start their employment with the AFM by means of an employment agreement or secondment agreement. This exception should be agreed in advance and individually with the compliance officer and included in the agreement.

1.3 Prohibitions

Insider trading is prohibited for anyone. This means AFM employees are not permitted to use inside information when carrying out private investment transactions and must avoid giving the appearance of insider trading. Moreover, it is prohibited to tip off others, give them recommendations or to induce them to trade with inside information.

Closed list and insider file

All employees having inside information at their disposal through their position need to disclose this in line with the 'Work instruction on updating the closed list' and/or require an insider file

in accordance with the 'Explanatory notes to insider files'. Both documents are available at Connect (AFM intranet).

AFM employees are prohibited from making private investment transactions in financial instruments issued by companies subject to the AFM's supervision. However, there are exceptions to this rule. Please consult the AFM licence registers to establish whether you are dealing with a company subject to the AFM's supervision.

Explanatory notes

Employees are not permitted to buy or sell any shares, bonds or derivative products, such as options, derivatives, turbos etc.:

- which are admitted to trading on a regulated market in the Netherlands. Nor may employees trade in these shares on other trading platforms.
- listed on a foreign stock exchange and supervised by the AFM. Consider issuers subject to the AFM's supervision and listed on a foreign stock exchange, for example. The AFM also supervises Dutch issuers' disclosures.

Crypto-assets are also included as financial instruments within the framework of this Regulation. Employees may only trade in cryptos issued by crypto-asset service providers that are not subject to the AFM's supervision. This does not concern the service provided by the crypto-service provider, but rather the crypto-assets issued by the crypto-service provider. If you are not sure whether a crypto is issued by a company subject to the AFM's supervision, please consult the AFM's public registry.

The risks of private investments are particularly high for AFM employees since the AFM has access to confidential data, for example data about companies subject to supervision. Confidential information is information that is not publicly available and use of which could lead to insider trading or the appearance thereof.

Circumventing the rules and confidentiality

Employees may not circumvent the rules of this Regulation by investing through third parties or by making investment recommendations (that are prohibited) to a third party.

Explanatory notes

The third parties described above could be the spouse or children, for example. However, it could also include the account of any association in which the employee holds an ancillary position. Employees may furthermore not instruct portfolio managers to perform transactions that are prohibited according to the Regulation.

Moreover, employees are also prohibited from any attempt to circumvent the rules by making indirect investments. Consider, for example, investments in the group of which the company subject to supervision forms part.

Employees must at all times comply with their duty to maintain confidentiality. Employees are also subject to a best-efforts obligation towards third parties whose investments need to be registered. Employees have to ensure those third parties' compliance with the rules as well.

1.4 Exceptions to the prohibition

As an exception to the prohibition, employees can perform the following private investment transactions: investment units in a collective investment company, subject to the condition that they do not exert any influence on the investment policy of the management company of the collective investment scheme or fund.

Explanatory notes

Participation rights in a collective investment scheme refer to an investment in a unit trust covered by an Undertaking for Collective Investment in Transferable Securities (UCITS) or that falls under an alternative investment fund manager (AIFMD Directive).

Exchange Traded Funds (ETFs), which are linked to an index, will be equated with unit trusts for the purpose of this Regulation.

Employees are allowed to accept dividends, such as stock dividend or optional dividend (cash or dividends in the form of shares). The transitional provision set out in 1.10 applies should employees receive shares subject to the prohibition via dividends.

Employees may invest or disinvest in projects via a crowdfunding service provider, except if they have supervisory information that could provide a potential advantage. If an actual or potential conflict of interest arises in holding investments in relation to their duties, employees must disclose this to the compliance officer without delay.

Employees are permitted to make investments under discretionary management agreements or in order to build up capital for a pension, mortgage or similar provision. This does require the compliance officer to assess in advance the discretionary management agreement and the agreement aimed at capital build-up for a pension, mortgage or similar provision. Employees must notify the compliance officer in advance before entering into these agreements, as well as in case of any interim changes.

The agreement must attest to the following:

- Employees will have no influence over the underlying investment policy that is pursued or the investment choices to be made by the manager or administrator (ownership and manager must be strictly separated); There will be no prior consultation between the portfolio manager and the employee and/or third parties regarding the investment transactions to be executed of which the investment needs to be disclosed.
- Employees have the option to issue generally worded policy instructions to the portfolio manager, for example in relation to the portfolio mix policy for financial instruments to be managed by the portfolio manager, by type, geographic origin or industry. These general policy instructions will have to be included in the agreement.

1.5 Disclosure of investments

Employees must register any investment accounts as soon as they enter service and/or open an investment account. The registration has to be complemented by:

- an agreement and an up-to-date overview of the
- portfolios:
 - in the employee's own name
 - in the name of minor children
 - a joint and/or investment account with the partner or a third party
 - investment accounts owned by the employee which are considered part of the community of property or registered partnership
 - third-party accounts for which the employee has been authorised and in which the employee holds a direct or indirect financial interest
 - an investment-linked mortgage, supplementary pension schemes with an investment component
 - investment-linked insurance and the portfolio under a discretionary management agreement
- the discretionary management agreement and a signed copy in case of interim changes thereof.

When it involves crypto-assets, employees must submit an overview of their crypto-assets issued by a crypto-asset service provider subject to the AFM's supervision.

At the compliance officer's request, employees are obliged to provide all information relating to private transactions carried out by or on behalf of the employee and/or those third parties of whom the account has to be registered.

1.6 Prevention of a conflict of interest of the members of the Executive Board and members of the Supervisory Board

This Regulation applies to each member of the Executive Board and each member of the Supervisory Board, subject to the exemptions which have received separate, prior approval from the compliance officer.

The transitional arrangement set out in 1.10 does not apply to members of the Executive Board and members of the Supervisory Board. Instead:

- a. Proposed directors for the Executive Board or the Supervisory Board must disclose their private investments and those of third parties of which the investments need to be disclosed to the compliance officer before they are nominated, appointed or re-appointed. See 1.5. The relevant private investments will be subject to a binding decision by the compliance officer as regards their acceptability.

In the event that the compliance officer determines in this binding decision that certain private investments are not acceptable, the decision will in any event mean that:

- The private investments must be divested before appointment to the Executive Board or the Supervisory Board; or
- The private investments must be placed under a discretionary management arrangement in accordance with 1.4 for the duration of the membership of the Executive Board or the Supervisory Board; or
- During membership of the Executive Board or the Supervisory Board, it will not be permitted to execute transactions in relation to the relevant private investments.

- b. Members of the Executive Board or the Supervisory Board who acquire a private investment after their appointment or re-appointment, for example by way of inheritance or as a gift,

must disclose this to the compliance officer immediately. The compliance officer will then issue a binding decision in respect of these private investments. See the conditions for eligibility under a. In this decision, the relevant member of the Executive Board or the Supervisory Board will be given a reasonable period of time to comply with the compliance officer's decision.

In order to avoid any potential or apparent conflict of interests, members of the Executive Board or the Supervisory Board cannot have any direct or indirect personal financial interests that are incompatible with membership of the AFM Executive Board or the AFM Supervisory Board. In these provisions, indirect financial interests are understood to mean the personal interests of third parties related to the member of the Executive Board or the Supervisory Board.

Direct or indirect financial interests will be incompatible with membership of the AFM Executive Board or the AFM Supervisory Board if those interests could result in:

- An actual or apparent conflict of interests and/or
- harm to the integrity, performance or reputation of the current or prospective relevant member of the Executive Board or Supervisory Board, or to the AFM.

In the event of a difference of opinion with the compliance officer regarding the interpretation and application of this Regulation, members of the Executive Board or Supervisory Board may refer the matter to the general counsel or the chair of the AFM Executive Board.

1.7 Disclosure requirement

Employees are required to make an immediate disclosure to the compliance officer in the event that:

- any of the provisions of this Regulation have not been complied with, either in full or in part, and/or
- a third party whose investments must be disclosed has made private investment transactions which are not permitted under this Regulation and/or
- the employee acquires a private investment, for example by way of inheritance or as a gift, which is subject to the prohibition. In such cases, the transitional provision applies.

Explanatory notes

If an actual or potential conflict of interest arises in holding investments in relation to the employee's duties, the employee must disclose this to the compliance officer without delay.

1.8 Compliance monitoring

The compliance officer is authorised to commission or carry out investigations into compliance with these provisions. Each year, the compliance officer will perform a risk-based monitoring. The employee in question is required to submit all information requested by the compliance officer.

1.9 Exemption authority of the compliance officer

In case of special personal or financial circumstances, the compliance officer may grant exemption from specific provisions of this Regulation. This exemption may be subject to requirements and restrictions.

The exemption authority covers special circumstances which involve financial instruments. Below refers to a number of special circumstances:

- Entering into or the dissolution of a marriage or registered

partnership (division of the property);

- Inheritance or acquisition from a gift or endowment;
- Termination of a mortgage or insurance contract with an investment element.
- Employees who have served more than three years in the permanent employment of the AFM may ask the compliance officer permission to sell their investment portfolio in a period to be determined by the compliance officer.

How to request for an exemption

The employee submits a request to the compliance officer for approval to be eligible for exemption. This request must state the reasons for the exemption. The employee must furthermore submit all information required by the compliance officer in order to assess the request, such as an up-to-date overview of the portfolio, the issuing company etc. Following a positive assessment, the compliance officer will notify the employee, stating the conditions that allow the aforesaid authorisation, if applicable. If in agreement, the employee confirms the aforementioned conditions.

1.10 Transitional provision

New employees who possess prohibited financial instruments as referred to in 1.3 before they take up employment with the AFM, have the option to sell these financial instruments within the first twelve months. In order to do so, the employee will need the compliance officer to grant pre-clearance.

Once the twelve-month period has elapsed, the employee will no longer be permitted to sell these financial instruments. The employee will not be permitted to execute transactions in these financial instruments again until two months after leaving the AFM's employment.

The entry into force of this Regulation will not affect the validity of any specific arrangements agreed between employees and compliance officers on the basis of the 2021 Regulation on private investment, unless otherwise notified by the compliance officer.

In those cases where this Regulation and the 2021 Regulation on private investment conflict, the compliance officer will establish a reasonable transitional regulation, if needed, with a maximum time limit of twelve months..

1.11 Binding ruling by the compliance officer and appeal

A decision taken, an exemption granted by the compliance officer or a ruling made by this officer regarding a request from an employee under these provisions is binding for the employee concerned.

Employees, including members of the Executive Board, can appeal to the chair of the AFM Supervisory Board against the compliance officer's decision or ruling. The chair of the Executive Board may lodge an appeal with the chair of the Supervisory Board. Members of the Supervisory Board are entitled to lodge an appeal with the chair of the AFM Executive Board. The chair of the Supervisory Board is entitled to lodge an appeal with the vice chair of the Supervisory Board.

The appeal has no suspensive effect on the decision or ruling of the compliance officer.

File management

The compliance officer registers all information obtained pursuant to this Regulation in the employee's compliance file.

Privacy

The compliance officer will treat any data and information received in connection with this Regulation as confidential at all times. Personal data processing in connection with the provisions in this Regulation will be carried out in accordance with the guidance provided in the General Data Protection Regulation (GDPR) and other applicable laws and regulations, and will be retained in accordance with the AFM data retention policy. More information on employees' privacy rights according to the GDPR are included in the in-house privacy regulations for AFM employees.

Residual powers

In all cases not provided for in this Regulation with respect to employees other than members of the Executive Board, a member of the Executive Board is empowered to adjudicate, issue instructions and take certain measures. With respect to members of the Executive Board or Supervisory Board, this authority rests with the chair of the Supervisory Board or, if the case concerns the chair of the Supervisory Board, the vice chair of the Supervisory Board.

Complaints procedure

In the event that an employee disagrees with the manner in which the Regulation has been implemented, they may submit a complaint to the AFM Complaints Committee. For further details, please refer to the AFM Complaints Procedure.

Entry into force

This regulation was revised in a number of respects and will enter into force on 1 May 2025.

Approval

This Regulation is adopted by the Executive Board and approved by the Supervisory Board, following the approval of the Works Council, if required.

Review and update

This Regulation is maintained and reviewed by the CIR manager, and revised, where needed. The review takes place once every three years or more often if warranted. Any material change passes to the Executive Board and Supervisory Board for approval and is communicated to the AFM employees.

Exceptions/deviations from the Regulation

All requests to deviate from the Regulation must be submitted to the owner, i.e. the CIR manager. Deviations from this Regulation will be recorded in writing, stating reasons.

2. The screening

2.1 Introduction

The AFM conducts screenings to ensure the reliability, integrity and suitability of current and prospective employees. The AFM's aim in doing so is to ensure the quality of its services and to hire employees who are reliable in performing their duties. The AFM also seeks to prevent that the position of an employee is or becomes such that their reliability and/or integrity might be called into question, thus contributing to the AFM's social mandate and a safe and healthy workplace culture. Screenings will be conducted before the start of the work (pre-employment screening) but may also be carried out in the course of an individual's employment (in-employment screening).

What is screening?

Screening means requesting information about the current or prospective employee. This is done to assess the individual's reliability, integrity and suitability. Based on the profile that emerges from these screenings, an assessment is made as to whether it is responsible to proceed with an employment agreement, or whether a reassignment to a different position or the engagement of an external professional is appropriate. Screening current and prospective employees may only be done if necessary and it needs to be proportionate as well relative to the risk sensitivity of the position. The level of screening depends on the position and nature of the employment.

The Human Resources & Facilities Division (HR & FB) and the Compliance, Integrity and Risk management division are particularly involved in the screening process.

Vulnerable positions

The AFM categorises certain roles as 'Vulnerable Positions' based on their sensitivity to risk. These are positions that entail additional risk of integrity breaches. Consider, for example, employees handling sensitive information or being in a position in which they find themselves particularly exposed. In the latter case, such positions include management positions (first-tier and second-tier positions), the role of general counsel, senior supervisors, compliance officers and fine officers.

2.2 Who does the Regulation apply to?

Seven categories of employees

The AFM will screen all prospective employees for reliability and suitability. The AFM has seven categories of current and prospective employees:

1. Individuals with whom the AFM has concluded an employment agreement;
2. Individuals who carry out work for the AFM on the basis of a secondment agreement or other agreement and have an AFM login account and/or access to confidential or highly confidential information;
3. Individuals who carry out work for the AFM on the basis of a secondment agreement or other agreement, who do not have an AFM login account and undertake scheduled tasks for the AFM on a structural basis and who do not have access to confidential or highly confidential information;
4. Individuals who carry out work for the AFM on the basis of a secondment agreement or other agreement, who do not have an AFM login account and undertake tasks for the AFM on an unscheduled and occasional basis and who do not have access to confidential or highly confidential information;

5. Individuals with whom DNB or another supervisory authority has concluded an employment agreement and who carry out work for the AFM on the basis of a secondment agreement or other agreement;
6. Individuals taking up the position as member of the Executive Board;
7. Individuals working in a position of trust.

For any employee who is assigned a different category after being screened, the screening will be restricted to those elements that did not form part of the previously conducted screening. An example could be an employee changing from category 2 to category 5.

Former employees

Prospective employees who were previously screened by the AFM and have not been out of its service for more than six months, will not be screened in full again, but will only be asked if there has been any change in their history. This exception from the screening will not apply if:

1. the individual confirms that there has been a change regarding their antecedents, or
2. if a category applies that is subject to a heightened level of screening.

If the first circumstance applies, the prospective employee will be subject to screening in full after all. If the second circumstance applies, the screening of the prospective employee will be restricted to those elements that did not form part of the previously conducted screening.

Notes to the seven categories: which screening?

Details per category are provided below. The screening moments are elaborated in 2.3.

Notes to category 1

The AFM carries out full screening for suitability and reliability for **prospective employees with an AFM employment agreement**. The

screening consists of a suitability screening which is performed by an external service provider. For this screening process the external service provider checks the employment history, validates degrees, reviews sanctions lists, contacts references, and obtains an integrity statement from the previous employer. The external service provider screens the factual data. The AFM performs a background check by requesting the judicial records, i.e. the criminal records. Furthermore, the AFM requests the prospective candidate to complete the so-called Reliability Questionnaire.

Moreover, the prospective candidate is requested to sign both a confidentiality agreement and the AFM Code of Conduct. The AFM also checks the prospective candidate's identity.

The Regulation on private investment and the statement of ancillary activities apply.

Notes to category 2

The AFM performs a full screening in respect of **prospective employees who will carry out work for the AFM on the basis of a secondment agreement or other agreement and have an AFM login account and/or access to confidential or highly confidential information**. This screening equals category 1, with the exception of the suitability element. The AFM performs a background check by requesting the judicial records, i.e. the criminal records. Furthermore, the AFM requests the prospective candidate to complete the so-called Reliability Questionnaire. Moreover, the prospective candidate is requested to sign a confidentiality agreement and the AFM Code of Conduct. The AFM also checks the prospective candidate's identity.

The Regulation on private investment and the statement of ancillary activities apply.

The AFM formulates the screening conditions in the procurement agreements for these employees. As a general rule, the supplier is charged with screening the suitability of the prospective employees. The supplier confirms that the screening took place prior to the start of the assignment and that it meets the AFM's requirements. The screening should principally comprise the same elements as were the

AFM to perform the screening itself, including those elements of the suitability screening at category 1, which involves elements such as the employment history, validation of degrees etc. CIR may be asked for its advice when drafting the procurement agreements.

This category inter alia covers employees of AFM's suppliers, such as consultancies, IT service providers, employment agencies, receptionists, security officers, the catering assistant manager, the catering manager and the catering cook. Interns with an intern agreement are also covered by category 2.

Notes to category 3

The AFM performs a limited screening for those **prospective employees who will carry out work for the AFM on the basis of a secondment agreement or other agreement, who do not have an AFM login account, no access to confidential or highly confidential information and who undertake scheduled tasks for the AFM on a structural basis**. The AFM does not screen the element of suitability. The AFM performs a background check by requesting the judicial records, i.e. the criminal records. Furthermore, the AFM requests the prospective candidate to complete the so-called Reliability Questionnaire. Moreover, these employees sign a confidentiality agreement and the AFM Code of Conduct on an individual basis. The AFM also checks the prospective candidate's identity.

The Regulation on private investment does not apply. The statement of ancillary activities does not apply.

The AFM formulates the screening conditions in the procurement agreements for these employees. As a general rule, the supplier is charged with screening the suitability of the prospective employees. The supplier confirms that the screening took place prior to the start of the assignment and that it meets the AFM's requirements. The screening should principally comprise the same elements as were the AFM to perform the screening itself, including those elements of the suitability screening at category 1, which involves elements such as the employment history, validation of degrees etc. CIR may be asked for its advice when drafting the procurement agreements.

This category includes non-company drivers, catering staff, cleaning staff, plant caretakers, work experience placements, amongst others.

Notes to category 4

The AFM performs a very limited screening for those **prospective employees who will carry out work for or at the AFM on the basis of a secondment agreement or other agreement, who do not have an AFM login account, no access to information and who undertake unscheduled and occasional tasks for the AFM** and who only have access to the AFM premises under supervision of the AFM. These employees each sign a confidentiality agreement and the AFM Code of Conduct on an individual basis. The AFM also checks the prospective candidate's identity.

The Regulation on private investment does not apply. The statement of ancillary activities does not apply.

The AFM formulates the screening conditions in the procurement agreements for these employees. As a general rule, the supplier is charged with part of the prospective employee's suitability screening. The supplier confirms that the screening took place prior to the start of the assignment and that it meets the AFM's suitability requirements. The screening should principally comprise the same elements as were the AFM to perform the screening itself, including those elements of the suitability screening at category 1, which involves elements such as the employment history, validation of degrees etc. The CIR may be asked for its advice when drafting the procurement agreements.

This category includes the staff of IT suppliers who do not have an AFM login account and no access to confidential or highly confidential information, mechanics and those on a work experience placement.

Notes to category 5

The AFM performs a very limited screening for those **prospective employees with whom DNB or another supervisory authority has concluded an employment agreement and who will carry out work for the AFM on the basis of a secondment agreement or other agreement**. These employees sign a confidentiality agreement and the

AFM Code of Conduct on an individual basis. The AFM also checks the prospective candidate's identity.

The Regulation on private investment applies. The statement of ancillary activities does not apply.

Notes to category 6

The secretary of the Supervisory Board handles the screening of a **prospective board member**. This is done according to a separate scheme. Prospective members of the Supervisory Board are also screened pursuant to category 6.

Notes to category 7

Separate rules apply to **prospective employees who are to take up a position of trust**. While the screening is not carried out by the AFM, it does initiate it. In exceptional cases, the minister can designate a specific position as a position of trust. A position of trust is in effect if it is possible to misuse knowledge or powers by virtue of the position, thereby compromising national security. Employees taking up a position of trust require a certificate of no objection ('verklaring van geen bezwaar', VGB). In order to obtain a VGB, the employee in question undergoes a security screening performed by the General Intelligence and Security Service (AIVD), also referred to as AIVD screening. This is done upon the AFM's request.

Overview

The paragraphs pre-employment screening and in-employment screening provide an overview of categories 1 through 5 as well as the screening elements.

2.3 When and how are screenings conducted?

Screening is conducted at the following moments in time:

Pre-employment screening

- Screening before a prospective employee starts their work for the AFM

In-employment screening

- Once every five years for all employees
- If an employee takes up a vulnerable position or another vulnerable position, or
- If antecedents, incidents and/or signals give cause for this.

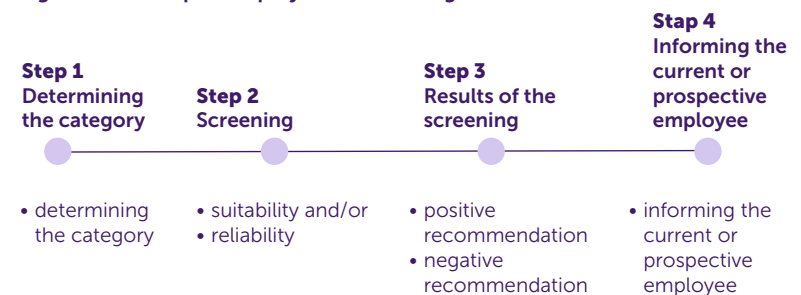
Pre-employment screening

Screening of prospective employees is a mandatory part of the recruitment process and the hiring of external staff and must be completed before the start of employment. The AFM makes use of an external service provider to perform part of the screening for category 1. This external service provider screens the factual data.

When it comes to criminal antecedents, the AFM has direct access to the information portal of the Judicial Information Service. This allows the AFM to request the prospective employee's extract. The AFM informs the prospective employee about this in advance. If there are any criminal antecedents, this will be stated in the extract. This only relates to criminal offences, such as fines for driving while under the influence. The AFM has no access to minor offences, such as fines for jumping a red light.

The figure below represents the process.

Figure 1. Proces pre-employment screening



Elements of pre-employment screening

The level of screening differs. The screening must be proportional, which means relative to the risk sensitivity of the position. The table below shows the elements screened for each category of prospective employee.

Table 1. Elements of pre-employment screening

Pre-employmentscreening	Wie	1	2	3	4	5
<i>Employment history</i>	SP	X				
<i>Degree validation</i>	SP	X				
<i>Sanctions list check</i>	SP	X				
<i>References check</i>	SP/AFM*	X				
<i>Integrity statement from previous employer</i>	SP	X				
<i>Background check (judicial records)</i>	AFM	X	X	X		
<i>Signing the confidentiality agreement</i>	AFM	X	X	X	X	X
<i>Signing the Code of Conduct</i>	AFM	X	X	X	X	X
<i>Identity check</i>	AFM	X	X	X	X	X
<i>Reliability Questionnaire**</i>	AFM					
<i>Criminal records check</i>		X	X	X		
<i>Investigation by supervisory authorities</i>	AFM	X1	X1	X1		
<i>Examination of other antecedents</i>	AFM	X	X			
<i>Other questions</i>	AFM	X	X			
<i>Regulation on Private Investment</i>	AFM	X	X			X
<i>Questionnaire regarding ancillary activities</i>	AFM	X	X			

Legenda

SP Externe service provider.

* Referentiencheck voor hoofden wordt uitgevoerd door de AFM, door senior recruiter of door een executive searchbureau.

** Zie voor een uitleg paragraaf 4.

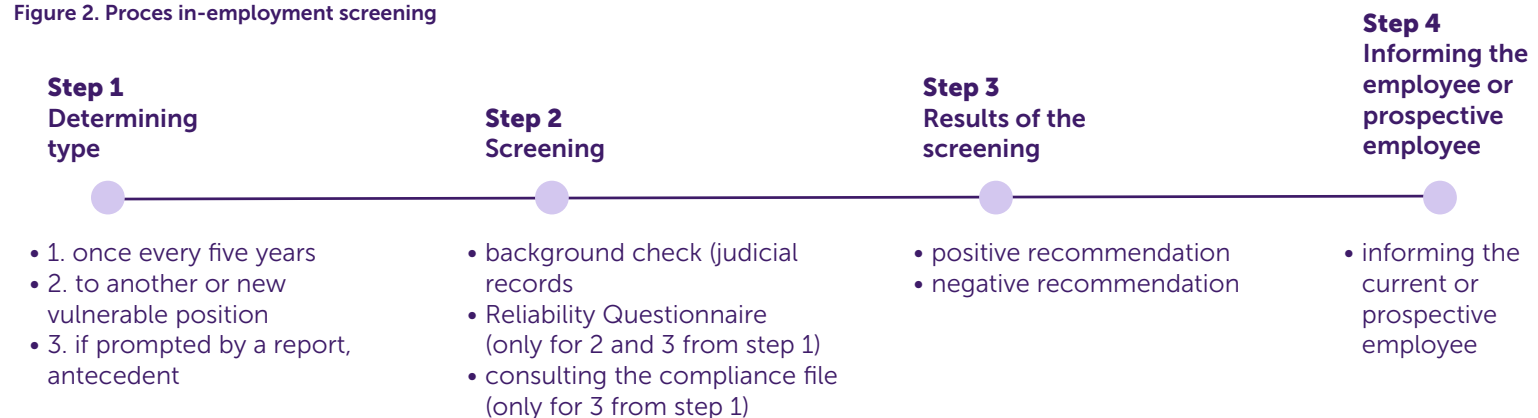
X1 Alleen voor kandidaat-medewerkers met een Kwetsbare functie.

In-employment screening

Current AFM employees can also be subject to screening. This is referred to as in-employment screening. This screening tests the reliability, which entails the following:

- **Once every five years** all category 1,2 and 3 employees (see 2.2) are re-screened. This screening tests the reliability and means the AFM runs a background check again (judicial records). Employees will be informed about this in advance.
- **If an employee decides to apply internally for a vulnerable position or for another vulnerable position**, and they are the last remaining candidate for the position and the last screening dates more than six months back, they will be screened again. This means that the employee will be asked to complete a new AFM Reliability Questionnaire. This questionnaire inquires about different types of antecedents and the AFM carries out a new background check (judicial records)
- **If antecedents or notifications give cause for it.** Antecedents or notifications may prompt an in-employment screening. This means that the employee will be asked to complete a new AFM Reliability Questionnaire. This questionnaire inquires about different types of antecedents. The AFM will also carry out a new background check (judicial records). Additionally, the compliance officer consults the compliance file.

Figure 2. Proces in-employment screening



Elements of in-employment screening

The table below shows the elements screened for each category of employee or prospective employee.

Table 2. In-employment screening

In-employment screening	Who	What
<i>Once every five years.</i>	<i>All category 1, 2 and 3 employees.</i>	Background check (judicial records).
<i>Transfer to a new or other Vulnerable Position</i>	If an employee applies internally for a vulnerable position or for another vulnerable position and they are the last remaining candidate for the position.	Reliability Questionnaire Background check (judicial records).
<i>In response to antecedents or reports.</i>	If prompted by an antecedent or report.	Reliability Questionnaire. Background check (judicial records) Consulting the compliance file.

2.4 Antecedents

The AFM Reliability Questionnaire may form part of the pre-employment screening and the in-employment screening. This questionnaire inquires about different types of antecedents. In terms of criminal antecedents, the law authorises the AFM to access judicial records for the purpose of a screening. See *Section 26 of the Decree on Judicial Information and Criminal Records*.

What antecedents should the current or prospective employee disclose?

The table below outlines the different types of antecedents, however, the list of examples must not be considered exhaustive. For each type of antecedent, current and prospective employees will find what must and what needs not be disclosed. Antecedents are a key factor in assessing the reliability of current and prospective employees. That is why it is crucial that antecedents are disclosed accurately, in full and without delay.

Criminal offences:

- *Things you must disclose:*
 - Crimes as provided for in the Dutch Criminal Code, the Opium Act, the Weapons and Ammunition Act, the Road Traffic Act, Property crimes and serious offences involving abuse of office, Sexual Offences Act.
 - Examples: Insider trading, tax fraud, embezzlement, physical abuse, vandalism, theft, driving whilst under the influence and failure to stop after an accident and sexual harassment.*
- *Things you do not need to disclose*
 - Minor offences; these are generally less serious in nature than crimes and are dealt with under administrative law. Examples: Traffic offences, such as exceeding the speed limit by up to 30 km/h, failure to wear a seat belt and public drunkenness.

Supervision

- Things you must disclose:
 - A company where your role includes involvement in or responsibility for policy setting has had a supervisory measure imposed, such as a warning or administrative fine.
- Things you do not need to disclose:
 - Supervisory measures do not need to be disclosed if your role did not include involvement in or responsibility for policy setting.

Other

- Things you must disclose:
 - Conflicts in the workplace that resulted in a measure such as a reprimand, warning, deduction of wages or dismissal. Employment, disciplinary or other similar measures imposed by a professional body, such as DSI or the Netherlands Bar Association.
- Things you do not need to disclose:
 - If a conflict in the workplace did not result in the imposition of a measure.

Weighting factors

Antecedents will be carefully assessed by the compliance officers using the following weighting factors: severity, culpability, time elapsed, disclosure, combination, capacity, attitude, motives and clarification.

Severity

To what extent does the antecedent impair the integrity with which the role could be fulfilled? One of the criteria used to determine the level of severity is the type of antecedent. These are classified in one of three categories.

Table 3. Examples of different types of antecedents.

(This list is not an exhausted list)

Severity	Category 1: minor (less severe)	Category 2: moderate (severe)	Category 3: major (very severe)
<i>Criminal record check</i>	<i>Maximum of two settlements with the Public Prosecution Service or fines for driving whilst under the influence.</i>	<i>Convictions for death or injury by negligence, failure to stop after an accident, theft, crimes of violence.</i>	<i>Convictions for economic crimes including forgery, fraud, extortion, embezzlement and convictions for offences against the Opium Act and tax legislation..</i>
<i>Supervision</i>	<i>Maximum of two warnings/ instructive meetings.</i>	<i>Providing incorrect or incomplete information to a supervisory authority. Measures imposed by a supervisory authority such as an administrative fine or an order subject to a penalty.</i>	<i>Measures imposed by a supervisory authority such as withdrawal of a license due to unethical management, report against the individual or company.</i>
<i>Other</i>	<i>Entry or warning as a result of a conflict in the workplace. Dismissal as a result of a conflict in the workplace.</i>	<i>Dismissal as a result of a conflict in the workplace. Disciplinary measures due to violation of integrity rules.</i>	

Although category 1 antecedents must still be disclosed to the compliance officer, they are in principle not considered grounds for further investigation, unless in the event of a repeat offence.

Culpability

Culpability centres on the extent to which the individual's behaviour was unethical and on whether or not they were aware of the immoral or illegal act or should they have been aware of it? Among other things, the level of culpability will be determined on the basis of attitude, capacity/position, intent (acting deliberately), intention and whether the offence is a repeat offence. If an individual has been fined multiple times for the same offence, this can point to an inadequate sense of values (and ability to learn). In such cases, a category 1 antecedent could be given significant weight.

Time elapsed

Time elapsed centres on the question how far back the antecedent took place. The more time has passed since an offence, the less weight will be given to it in assessing reliability.

To ensure that past antecedents do not stand in the way of a current or prospective employee's future for too long, in its assessment, the AFM applies a five-year period for minor and severe antecedents. For major antecedents, the AFM proceeds from a period up to ten years. If the individual to be assessed has had an extended period without any antecedents prior to a screening or re-screening, they must be able to continue with a 'clean slate'.

This means that any antecedents dating back more than ten years are not taken into consideration, unless:

- the facts at issue are very serious and potentially relevant to the intended position at the AFM, category 3 antecedents and/or related to a repeat offence, category 3¹ antecedent.
- In consultation with the CIR manager, the compliance officer decides whether this is the case at hand.

Combinatie

If multiple antecedents exist, these will be assessed in relation to each other. This could mean that an antecedent that does not qualify as severe on its own merits could still give rise to doubts as regards the employee's reliability when considered in combination with other antecedents.

Capacity

Was the person acting in a professional or private capacity at the time of the antecedent? Could the antecedent be attributed to youthful indiscretion (applicable up to and including the age of 25)? Other relevant aspects for the weighting can be the individual's position, education or professional background.

Disclosure

Did the individual ensure the antecedent was disclosed by themselves and without delay (mitigating circumstance) or not, in which case this counts as an aggravating circumstance? In the event an antecedent was not disclosed, it will be checked whether the information was deliberately withheld. The deliberate withholding of information is given great weight.

Attitude, motives and clarification

Does the individual recognise how serious their action or failure to act was and that the antecedent should not have happened? The answer to that question, too, could be relevant for the assessment, as is a cooperative stance. An appropriate attitude, plausible motives and extensive clarification may count as mitigating circumstances.

1 Category 3 antecedents are severe (extremely serious)

2.4.1 The assessment of antecedents

The compliance officer assesses antecedents at HR & FB's request. The assessment is based on the weighting factors described above. In this assessment, not all antecedents will be accorded the same weight. Failure to come forward about an antecedent may be factored into the assessment as an aggravating circumstance. This could raise doubts about the reliability, even if the antecedent itself does not carry great weight. This is why it is important to always be open and honest.

In case any additional information is needed or if there is any doubt, the compliance officer will usually enter into consultations with the employee or prospective employee. For the purposes of the assessment, the four-eye principle is always observed as a minimum. If the conclusion is positive, this means there is agreement with a fellow compliance officer. In case of any doubt, the conclusion is also presented to the CIR manager. The CIR manager decides. The compliance officer communicates the positive or negative outcome to HR & FB. HR & FB is not informed about the contents of the antecedents and/or the assessment thereof.

Change in antecedents

As stated in the Code of Conduct all AFM employees in employment have to disclose any changes in their antecedents. In the event that there is a change in antecedents the disclosure and employee statements in respect of antecedents will be added to the in-house system by employees themselves. The compliance officer will assess and communicate and manage all disclosures made by employees relating to any changes in antecedents. If the antecedent raises any questions about that individual's reliability the disclosure may prompt an in-employment screening and further investigation. Examples of such antecedents include involvement with criminal antecedents such as fraud or theft. On the other hand fines for matters such as driving while under the influence or inaccuracies in a declaration do not necessarily result in in-employment rescreening unless the offence is a repeat offence. More information on antecedents and their weighting is provided in Paragraph 2.4. Changes in the employee's antecedents may result in the imposition of a sanction. See the Regulation on Sanctions.

2.5 Consequences of the screening's outcomes

Pre-employment screening

The AFM will take into account all facts and circumstances to assess the reliability, integrity and suitability of a prospective employee. The employee concerned will be informed about the outcome of the screening prior to entering into employment. The contact within HR & FB will inform the prospective employee of this decision.

If the assessment results in a negative recommendation, HR & FB will notify the employee of the outcome of the screening. The following outcomes of a screening may lead to the decision whether or not to appoint a prospective employee. For example:

- In the event that inaccuracies have been identified in the screening process, for example in terms of qualifications or employment history.
- If prompted by the assessment of antecedents.

The outcome may also lead to a meeting with the compliance officer. In that case, topics include the reliability, taking additional measures or the matter of whether the employment will be entered into or terminated. If requested, the compliance officer will give an explanation to the prospective employee about the outcome of the antecedents assessment.

In-employment screening

The findings of in-employment screening can sometimes lead to a meeting with the compliance officer. Should the assessment lead to a negative outcome in terms of reliability, this may give cause to measures, or termination of the employment. The sanctions are described in the Regulation on sanctions.

Delegation of duties

Within the AFM, the following divisions are involved in and responsible for the screening.

Pre-employment screening

HR & FB

- Organising the screening process and executing the screening of prospective employees

Executive office

- Organising the screening process and executing the screening of prospective members of the Executive Board and prospective members of the Supervisory Board

- Access to systems

FB

- Access to physical areas

CIR

- Assessing criminal and other antecedents and hits on sanctions lists
- Conducting interviews with prospective employees if needed for the assessment
- Advising HR & FB on the reliability of a current or prospective employee
- Assessing ancillary activities
- Assessing investment accounts

The responsibility for organising and executing screenings for prospective members of the Executive Board or members of the Supervisory Board rests with the secretary for the Supervisory Board. If any antecedents are identified, the secretary will request a recommendation of CIR.

In-employment screening

HR & FB

- Executing the screening and organising the associated process

In the event that the screening reveals any antecedents, a compliance officer will be asked to assess these and advise HR & FB on the reliability of the employee.

CIR

- Assessing criminal and other antecedents

- Conducting one or more interviews regarding the antecedents with the employee in case of an incident or signal
- Providing HR & FB a mandatory recommendation on the reliability of the employee.
- The compliance officer assesses the need for an in-employment screening in case of a report or change in the antecedent.

File management

All relevant documents and the considerations made in the screening process are recorded in the personnel file. The personnel file is maintained by HR & FB. The information stored in the personnel file on any measures could have consequences for employees who apply for a position with another employer, should this employer conduct a reference check and request an integrity statement from the AFM.

Privacy

The compliance officer and HR & FB will treat any data and information received in connection with this Regulation as confidential at all times. Personal data processing in connection with the provisions in this Regulation will be carried out in accordance with the guidance provided in the General Data Protection Regulation (GDPR) and other applicable laws and regulations, and will be retained in accordance with the AFM data retention policy. More information on current and prospective employees' privacy rights according to the GDPR are included in the privacy statement for prospective employees and the in-house privacy regulations for AFM employees.

Residual powers

In all cases not provided for in this Regulation with respect to employees other than members of the Executive Board, a member of the Executive Board is empowered to adjudicate, issue instructions and take certain measures. With respect to members of the Executive Board or members of the Supervisory Board, this authority rests with the chair of the Supervisory Board or, if the case concerns the chair of the Supervisory Board, the vice chair of the Supervisory Board.

Complaints procedure

In the event that an employee disagrees with the manner in which the Regulation has been implemented, they may submit a complaint to the AFM Complaints Committee. For further details, please refer to the AFM Complaints Procedure.

Entry into force

This Regulation was revised in a number of respects and will enter into force on 1 May 2025.

Approval

This Regulation is adopted by the Executive Board and approved by the Supervisory Board, following the Works Council's consent, if required

Review and update

This Regulation is maintained and reviewed by the head of HR & FB, and revised, where needed. The review takes place once every three years or more often if warranted. Any material change passes to the Executive Board for approval and is communicated to the AFM employees.

Exceptions/deviations from the Regulation

All requests to deviate from the Regulation must be submitted to the owner, i.e. the head of HR & FB. Deviations that concern the classification, antecedents, private investments and ancillary activities are submitted to the CIR manager. Deviations from the Regulation will be recorded in writing, stating reasons.

3. The regulation on reporting apparent or suspected wrongdoings, violations of integrity and undesirable behaviour

3.1 Introduction

Integrity has the AFM's utmost priority. For this reason, the AFM promotes a strong culture in which wrongdoings, integrity violations and undesirable behaviour have no place. Should they nonetheless occur, there must be a safe and quick way to report wrongdoings or integrity violations, so that action can be taken. This Regulation describes the safe ways in which we at the AFM can report apparent and suspected integrity violations, undesirable behaviour and wrongdoings to the in-house hotline. The Regulation on integrity investigations pertains to the assessment of reports and the ways in which an investigation is carried out.

What constitutes a violation of integrity?

An integrity violation is an incident during which an employee fails to comply with laws, internal regulations and the AFM's values and standards. Integrity violations can take many forms. Examples include involvement with criminal offences such as fraud or theft. Internal regulations may relate to non-compliance with rules involving ancillary activities, non-compliance with the Regulation on private investment or rules governing the acceptance of gifts and invitations. A breach of the duty to maintain confidentiality is also an example of an integrity violation. Integrity violations may also comprise undesirable behaviour.

What constitutes undesirable behaviour?

Undesirable behaviour is behaviour that is perceived as crossing a line or offensive, which is intended to make an employee no longer feel safe at their place of work, or has the effect of doing so. This may include discrimination, aggression and violence and harassment, sexual or otherwise.

What constitutes a wrongdoing?

Wrongdoings fall into two categories:

- a breach of Union law: a breach of a regulation or directive of the European Union in specific policy areas.
- a societal wrongdoing.

What constitutes a breach of Union law?

A breach of Union law is an act or omission that is unlawful or undermines its objective. This concerns acts of the European Union, i.e. EU regulations or directives, or national legislation and regulations derived from them, within certain policy areas. A full list of relevant policy areas is provided in Annex 2 of the Directive². Examples include environmental protection or the protection of personal data.

² See Annex 2 of Directive (EU) 2019/1937 of the European Parliament and the Council of 23 October 2019 on the protection of persons who report breaches of Union law.

What constitutes a societal wrongdoing?

Societal wrongdoing occurs when an act or omission affects the public interest. Such an act or omission must display one or more of the following characteristics:

- it involves a violation of the law or of internal rules established by the AFM pursuant to a statutory provision.
- there is a threat to public health
- there is a threat to the safety of individuals
- there is a risk of environmental degradation
- there is a threat to the proper functioning of the organisation as a result of an improper act or omission.

The hotline can assess for each individual case whether it constitutes a matter of public interest. Social interest is, in any case, deemed to be at stake if:

- the act or omission affects more than just personal interests and individuals and
- involves either a pattern or structural issue, or
- if the act or omission is serious or extensive in nature.

This Regulation is not intended for personal grievances in relation to conflicts between employee and manager or similar matters. Should this be the case, employees can best turn to HR & FB or one of the confidential counsellors. This Regulation also differs from the AFM Complaints Procedure. The AFM Complaints Procedure is open to anyone who wishes to submit a complaint regarding any act and/or failure to act by the AFM and its employees. See the AFM website: [Complaint about the AFM](#).

3.2 Who does the Regulation apply to?

The Regulation applies to anyone who works, will work, or has worked at the AFM, as well as all individuals who have had, currently have, or will have contact with the AFM in a professional or work-related capacity. This includes all internal and external employees of the AFM, including interns and volunteers, as well as job applicants and suppliers.

3.3 What can be reported?

This Regulation provides employees with a possibility to report apparent and suspected integrity violations, undesirable behaviour and wrongdoings involving the AFM.

The overview provides a number of examples but this is not an exhaustive list.

Table 4. reporting apparant or suspected wrongdoing, violations of integrity and undesirable behaviour

Examples of apparent or suspected integrity violations	Examples of apparent or suspected undesirable behaviour	Examples of apparent or suspected wrongdoings
<ul style="list-style-type: none"> • <i>Conflict of interests (e.g. undesirable ancillary activities).</i> • <i>Theft, fraud</i> • <i>Economic offences, such as tax fraud, forgery, embazzlement and bribery</i> • <i>Insider trading</i> • <i>Deliberately leaking confidential supervisory information</i> • <i>Misuse of information and/or powers interests</i> 	<ul style="list-style-type: none"> • <i>Discrimination</i> • <i>Agression and violence/intimidation</i> • <i>Bullying</i> • <i>Sexsual harassment</i> • <i>Excluding or ignoring</i> 	<ul style="list-style-type: none"> • <i>Breaches of Union law, in which case it refers to the violation of specific directives or regulations covering specific areas. These include health, protection of personal data or security of network systems and information systems.</i> • <i>Social interest is deemed to be at stake; the act or omission affects more than personal.</i>

3.4 Internal reporting – where to report?

Apparent or suspected integrity violations, undesirable behaviour or wrongdoings may be reported verbally or in writing to:

- the hotline, consisting of the compliance officers.
- the hotline can be contacted via e-mail: compliance@afm.nl or via the [Reporting form – Portal \(afm.nl\)](#).
- you can report to your line manager, another line manager or senior line manager within the AFM
- the chair of the Executive Board.

The line manager or the chair of the Executive Board will make an initial assessment and submits the report in confidence to the hotline as soon as possible. The hotline determines whether or not the report is covered by the Regulation. In all other cases, the line manager will handle the report themselves.

Explanatory notes

The hotline assesses the report as described in the Regulation on integrity investigations. There may be an interview with an HR adviser if the report relates to undesirable behaviour. Possible solutions may include a meeting or a corrective interview, mediation, submitting a complaint or initiating an internal investigation.

The reporting individual can also ask one of the confidential counsellors to submit a confidential report to the hotline on their behalf. In that case, the reporting individual's contact details will only be known to the confidential counsellor, and not to the rest of the organisation.

Reports relating to the performance and/or conduct of the Executive Board may also be submitted to the chair or members of the AFM Supervisory Board. The person receiving the report will inform the hotline.

Reports relating to the performance and/or actions of members of the Supervisory Board or the chair of the Supervisory Board,

may also be submitted to the chair of the Supervisory Board or the vice chair of the Supervisory Board, respectively. The person receiving the report will inform the hotline.

The hotline will confidentially and immediately inform the chair of the Executive Board of the report of the apparent or suspected wrongdoing.

If the report involves an integrity violation, including undesirable behaviour, the hotline will inform the CIR manager thereof.

The hotline will inform the chair of the Supervisory Board of any reports received by the hotline that pertain to the Executive Board's actions. With respect to reports relating to the actions of the members of the Supervisory Board or one of its members, the hotline will inform the chair or the vice chair of the Supervisory Board.

3.5 Confidentiality

The hotline will not disclose the reporting individual's identity, unless the reporting individual agrees to the disclosure of their identity. In providing information, the reporting individual's identity will not be revealed. Information that could identify the reporting individual either directly or indirectly will only be shared with the reporting individual's consent or if the law requires this, for example, if there is a statutory duty to report.

3.6 Anonymous reporting

It is also possible to make a report anonymously. Should employees wish to make an anonymous report, they can do so via the [Reporting form – Portal \(afm.nl\)](#).

Reports can be submitted anonymously but will only be taken into consideration if they are sufficiently specific to enable further investigation. The preferred option is to report anonymously via the confidential counsellor, given that the confidential counsellor will be able to ask those questions needed to make a case sufficiently specific.

It also allows those assessing the report to put questions to the confidential counsellor, if needed.

3.7 Informatie en advies voor de melder

The reporting individual has the option to discuss issues in confidence with a confidential counsellor of the AFM. Confidential counsellors are independent, and will listen and provide advice and information to the reporting individual.

The reporting individual may also seek advice from others in confidence, such as an external consultant, a lawyer, a lawyer from a trade union or legal-aid insurance company or the company doctor. These people can advise the reporting individual on how best to make the report. They can also alert the reporting individual to the risks of reporting.

The AFM may reimburse the cost of an external adviser up to a reasonable amount, which the Executive Board will decide on.

In case of actual or suspected wrongdoing, the reporting individual is also able to obtain information, guidance and support from the external advisory team of the Dutch Whistleblowers Authority (Huis voor Klokkenluiders).

3.8 Recording of reports and confirmation of receipt

In the case of a verbal report, the hotline will document the report and the date of receipt in writing and, within seven calendar days of the report, provide the reporting individual with the opportunity to check, correct and sign the record of the conversation for approval. A copy of this will be sent to the reporting individual.

For reports submitted in writing, the reporting individual will receive a confirmation of receipt from the hotline within seven calendar days.

The hotline records the report in a report register set up for this purpose.

3.9 Handling of the report

The hotline completes an initial assessment of the report. See the Regulation on integrity investigation. The hotline assesses whether the report is covered by the Regulation. If the report is not covered by the Regulation, the hotline will inform the reporting individual about this.

If the report involves an apparent or suspected wrongdoing, the chair of the Executive Board will decide in consultation with the hotline whether this gives cause for an investigation.

With regard to reports of a potential violation of integrity, the decision whether or not to investigate will be taken by the CIR manager in consultation with the hotline. In case of a serious integrity violation, this decision may be taken in consultation with the head of Legal Affairs, the head of HR & FB, the general counsel and/or the chair of the Executive Board.

If the report relates to potential undesirable behaviour, the decision as to whether or not to investigate the matter in accordance with the Regulation on integrity investigation, or whether the report will be followed up in accordance with the Regulation on complaints related to undesirable behaviour will be made in consultation with the reporting individual. Above section applies in the event of an investigation.

The decision as to whether or not to launch an investigation is made by the chair of the Executive Board if the CIR manager or a CIR employee could be involved in an apparent or suspected wrongdoing or integrity violation, including undesirable behaviour.

With regard to apparent or suspected wrongdoings or integrity violations, including undesirable behaviour, which could involve a member of the Executive Board, the decision whether to investigate will be taken by the chair of the Supervisory Board.

In cases of apparent or suspected wrongdoings or integrity violations, including undesirable behaviour that could involve the chair of the Supervisory Board, the vice chair of the Supervisory Board will be authorised to launch an investigation.

Investigations are carried out by an independent investigative team. This team has special security-related obligations and obligations in relation to confidentiality. This team can either be an in-house team or an external team.

In reports about undesirable behaviour, the general counsel will also be involved in the investigation, if needed.

External advice may be sought and/or external investigation may be conducted in the following situations: if the report concerns any employees from CIR, if the report involves the Executive Board or members of the Supervisory Board, if the report relates to an apparent or suspected wrongdoing with major social implications, if the preferred expertise about the topic is lacking, in case of preferred independence and impartiality or due to insufficient in-house capacity.

3.10 Informing the reporting individual

The hotline will notify the reporting individual about the outcome no later than six weeks following the date of receipt of the report made by the reporting individual. If possible, the hotline will also provide an account of the steps the report has led to, such as measures taken or planned, unless there are compelling reasons not to do so.

Even if it were to be decided that no further action will be taken on the report, the reporting individual will be informed of this, including the reason for that decision.

The reporting individual will receive notification if it does not prove possible to give the outcome within six weeks. The reporting individual will also be informed in writing of the timeframe within which they will as yet receive the outcome. The reporting individual will not be notified regarding the progress and/or the outcome of the investigation if such information could compromise the investigation or legal proceedings.

3.11 Reporting a suspicion of wrongdoing externally

It is possible to report a wrongdoing or a suspicion of wrongdoing internally, however, it is also possible to directly file an external report. This option is made possible by the Whistleblowers Protection Act. However, this act does not foresee in the option of direct external reporting on apparent or suspected integrity violations or undesirable behaviour. These can only be reported internally.

The reporting individual can make an external report of an apparent or suspected wrongdoing to a competent external authority. Those authorities are included in the list of definitions.

3.12 Legal protection

Legal protection for the reporting individual

Individuals reporting an incident in good faith and showing due care will have their legal position protected during and after the handling of a report. Consequently, reporting individuals may not be disadvantaged during and after the handling of a report. Such detriment may include a dismissal, temporary agreements not being extended, bullying or suddenly receiving negative performance reviews. Detriment also covers the threat of being disadvantaged as well as any successful or failed attempt at disadvantaging the reporting individual. The aforementioned legal protection is subject to the condition that the reporting individual has reasonable grounds, supported by facts, to believe that the information regarding the report is accurate at the time of reporting and that the report has been made in accordance with this Regulation.

Protection for other concerned parties

The legal status of individuals involved in the report is also protected. This for example refers to external advisers, confidential counsellors, any witnesses of incidents acting in good faith, the hotline and the in-house or external investigators. This means that they will not be affected in any way whatsoever as a result of their involvement. However, it is essential that individuals act in good faith; otherwise, they are not afforded legal protection.

Third parties, colleagues and family members of the reporting individual are also protected if they are in a working relationship with the individual who is the subject of the report.

Accused individuals will also have their legal position protected. This means the accused will be deemed innocent until proven otherwise and their position will not be affected in any way whatsoever until such proof is found.

Protection after public disclosure of apparent or suspected wrongdoing

Public disclosure, for example, means going to the press. Being entitled to protection before and after the report requires certain conditions having to be met. These are set out below.

Protection if no report has been made yet

The protection in case of public disclosure of an apparent or suspected wrongdoing applies if there is no report yet and the reporting individual has reasonable grounds to believe that:

- Information reported on a wrongdoing is correct at the time of disclosure, and
- The wrongdoing may be a threat or realistic danger to the general public interest, or
- There is a risk of detriment when reporting to a competent authority, or other competent body, or
- It is unlikely that the wrongdoing will be adequately addressed.

The protection means that reporting individuals may not be disadvantaged during and after the handling of a report.

Protection if the report was made to a competent authority

The protection in case of public disclosure of an apparent or suspected wrongdoing against detriment applies if the reporting individual made the report to an external competent authority (and possibly to the AFM prior to that) subject to the following conditions:

- The reporting individual has reasonable grounds to assume that the information reported on an apparent or suspected wrongdoing is correct at the time of the public disclosure, and
- The reporting individual has reasonable grounds to assume that the investigation is not making sufficient progress, based on the information provided by the competent authority to which the reporting individual has submitted the report or follow-up of the report.

The protection means that reporting individuals may not be disadvantaged during and after the handling of a report.

Should a reporting individual consider to publicly disclose their report, they are advised to first contact a confidential counsellor, as the conditions for the protection of reporting individuals when publicly disclosing reports are complicated. The confidential counsellor can explain the route to be followed.

The post-disclosure protection also applies to employees who support the reporting individuals and to other concerned parties.

Detriment

Should a reporting individual nevertheless find that they are being disadvantaged after all due to their report of an apparent or suspected wrongdoing, they can request the Dutch Whistleblowers Authority (Huis voor Klokkenluiders) to investigate the matter. The reporting individual can also initiate legal proceedings. In that case, it is up to the reporting individual to demonstrate that they reported a wrongdoing or a suspicion of wrongdoing and that this has led to detriment. In

legal proceedings, the court will assume that the detriment resulted from the report. The AFM will then have to prove that this was not the case.

Indemnification in legal proceedings

The reporting individual is protected against any legal action due to a report or for publicly disclosing a wrongdoing, even if this means that the duty to maintain confidentiality is breached. This applies provided the reporting individual reasonably thought that the disclosure was a necessary action and that the report or the public disclosure of the wrongdoing has proceeded as outlined in this Regulation.

This indemnification also applies to those individuals who support the reporting individual and to other concerned parties.

3.13 Misuse of the Regulation

Any misuse of this Regulation, including reports made in bad faith, may result in disciplinary measures or legal proceedings. Anyone responsible for the adverse treatment of a reporting individual will be subject to the same sanctions.

Delegation of duties

Within the AFM, the following officials are involved in and responsible for the assessment and follow-up of reports and for launching investigations:

Hotline

- Implementing the hotline and keeping a report register
- Assessing the reports (triage)
- Liaising with the reporting individual
- Providing advice on investigations that may or may not be initiated for the CIR manager in case of apparent or suspected integrity violations or undesirable behaviour or for the chair of the Executive Board in case of apparent or suspected wrongdoings or serious integrity violations or undesirable behaviour.
- Monitoring the progress and deadlines of the reporting procedure and the investigation procedure.
- Insight into the development of the nature and extent of the integrity violations and reports.

Confidential counsellors

- Offering a sympathetic ear to the reporting individual
- Passing on the report on behalf of the reporting individual should the reporting individual specifically request this.

CIR Manager

- Making a decision on whether or not to launch a regular or special investigation when it involves an integrity violation or undesirable behaviour. In case of a serious integrity violation or undesirable behaviour, the CIR manager may consult with the head of HR & FB, the head of Legal Affairs, the general counsel and/or the chair of the Executive Board.

Line managers

- Receiving reports and passing them on to the hotline.

Chair of the Executive Board

- Receiving reports and passing them on to the hotline.
- Making a decision on whether or not to launch a regular or special investigation when it involves an apparent or suspected wrongdoing.
- Making a decision on whether or not to launch a regular or special investigation in cases involving the CIR manager or a CIR employee in an apparent or suspected wrongdoing or integrity violation.

Chair of the Supervisory Board

- Receiving reports about a member of the Executive Board and passing them on to the hotline.
- Making a decision on whether or not to launch a regular or special investigation when it relates to an apparent or suspected wrongdoing or integrity violation involving a member of the Executive Board.

Members of the Supervisory Board

- Receiving reports about a member of the Executive Board and passing them on to the hotline.

Vice chair of the Supervisory Board

- Making a decision on whether or not to launch a regular or special investigation when it relates to an apparent or suspected wrongdoing or integrity violation involving a member of the Supervisory Board.

General counsel

- May join the investigative team if the report relates to undesirable behaviour.

File management

The hotline records reports in a report register set up for this purpose in a secure environment.

Privacy

The hotline will treat any data and information received in connection with this Regulation as confidential at all times. Personal data processing in connection with the provisions in this Regulation will be carried out in accordance with the guidance provided in the General Data Protection Regulation (GDPR) and other applicable laws and regulations, and will be retained in accordance with the AFM data retention policy. More information on employees' privacy rights according to the GDPR are included in the in-house privacy regulations for AFM employees.

Residual powers

In all cases not provided for in this Regulation with respect to employees other than members of the Executive Board, a member of the Executive Board is empowered to adjudicate, issue instructions and take certain measures. With respect to members of the Executive Board or members of the Supervisory Board, this authority rests with the chair of the Supervisory Board or, if the case concerns the chair of the Supervisory Board, the vice chair of the Supervisory Board.

Complaints procedure

If the reporting individual or another concerned party disagrees with the manner in which the Regulation has been implemented, they may submit a complaint to the AFM Complaints Committee. For further details, please refer to the AFM Complaints Procedure.

Entry into force

This Regulation was revised in a number of respects and will enter into force on 1 May 2025.

Approval

This Regulation is adopted by the Executive Board and approved by the Supervisory Board, following the Works Council's consent, if required.

Review and update

This Regulation is maintained and reviewed by the CIR manager, and revised, where needed. The review takes place once every three years or more often if warranted. Any material change passes to the Executive Board and Supervisory Board for approval and is communicated to the AFM employees.

Exceptions/deviations from the Regulation

All requests to deviate from the Regulation must be submitted to the owner, i.e. the CIR manager. Deviations from this Regulation will be recorded in writing, stating reasons.

Summary of the reporting regulation - When, to whom and how to report

Do you suspect undesirable behaviour?

Together, we create a safe and healthy working environment that embodies integrity. The AFM does not tolerate undesirable behaviour and aims to protect its employees from this. Should you unexpectedly encounter undesirable behaviour, the preferred approach is to first attempt to address and resolve undesirable behaviour with the offending party. You can also approach your line manager, the HR adviser or a confidential counsellor.

If your attempts are unsuccessful, or if the nature of the conduct and/or relationship is such that raising the issue is not an option, you could submit a report with the in-house hotline. See below at Report it internally. Together, we will figure out the next steps.

Do you suspect a violation of integrity or wrongdoing?

The AFM aims to offer a safe work environment and a safe reporting environment. Anyone at the AFM should feel free to report apparent and suspected wrongdoings and integrity violations. This will not always be easy, in particular if you have any direct or indirect involvement yourself, or if an abuse or breach concerns you. You should preferably submit your report internally. This is because the primary responsibility for addressing a breach or wrongdoing rests with the AFM.

The preferred approach is for you to report it internally so that we can solve it internally. However, you do not need to make an internal report first. You could also directly report suspicions of any wrongdoing externally. It is not possible to file direct external reports of apparent or suspected integrity violations or undesirable behaviour.

Anonymous reporting

It is also possible to make an anonymous report. However, be aware that there need to be sufficient specific starting points for the AFM to follow up on an anonymous report. It may be wise to report through an intermediary, as this allows for the option to ask clarifying questions at a later date.

Table 5. Reports

Report	Report it internally		Report it externally
What to report?	Apparant or suspected integrity violations or wrongdoing.	Apparent or suspected undesirable behaviour.	Apparant or suspected wrongdoing.
Where to report?	In-house hotline (compliance officers) compliance@aafm.nl your line manager or the chair of the Executive Board. Or via the Reporting form - Portal (aafm.nl); You will receive an acknowledgement of receipt from the hotline within seven calendar days.		A competent authority.
Need help?	Please contact an external or in-house confidential counsellor or an external adviser. Suspicions of wrongdoing can also be submitted to the Consultation Department of the Dutch Whistleblowers Authority (Huis voor Klokkenluiders).		Please contact an external or in-house confidential counsellors, external adviser or of the Dutch Whistleblowers Authority (Huis voor Klokkenluiders).
Initial assessment of the report	<p>The hotline will inform you as soon as possible about the initial assessment of the report.</p> <p>If the report relates to apparent or suspected undesirable behaviour, the decision will be made in consultation with you as to whether the report will be handled according to the reporting procedure or the complaints procedure.</p> <p>If the decision is made to opt for the complaints procedure, the hotline will pass on the complaint to the chair of the Complaints Committee. The Complaints Committee will send you a written acknowledgement of receipt within seven calendar days following the receipt of the complaint from the hotline.</p>		
Start of the investigation	<p>The hotline informs you and any other concerned parties whether an investigation will be launched.</p> <p>The competent body will decide on the starting date of an investigation.</p>	<p>The Complaints Committee informs you and the accused whether an investigation will be launched.</p> <p>The Complaints Committee will decide on the starting date of an investigation.</p>	

Report	Report it internally	Report it externally
<i>Who carries out the investigation?</i>	<i>An in-house or external investigation team, or a combination thereof.</i>	<i>An in-house or external investigation team, or a combination thereof.</i>
<i>Giving both sides the opportunity to present their case.</i>	<i>You and any other concerned parties will be heard. Both sides will be given the opportunity to present their case.</i>	<i>You and the accused and any parties concerned will be heard. Both sides will be given the opportunity to present their case.</i>
<i>Recommendation by the Complaints Committee</i>	<i>Not applicable</i>	<i>The Complaints Committee will submit an opinion to the chair of the Executive Board no later than six weeks following the receipt of the complaint.</i>
<i>Draft report</i>	<i>You will be given the opportunity to respond to the draft report, drawn up by the investigative committee, unless there are compelling reasons against this.</i>	
<i>Decision and consequences</i>	<i>The hotline will inform you within six weeks after you have received the confirmation of receipt about the steps that have been taken in response to your report, unless there are compelling reasons not to do so.</i>	<i>The Chair of the Executive Board will take a decision about the complaint, and any measures to be imposed within twelve calendar days, following the receipt of the Complaints Committee's recommendation.</i>

You can expect the AFM to treat your report with due care. All communication is handled in the strictest of confidence. For more information, please read the Code of Conduct and the Regulation on reporting apparent and suspected wrongdoings, integrity violations and undesirable behaviour.

4. The regulation on integrity investigations

4.1 Introduction

Reports relating to apparent or suspected integrity violations, undesirable behaviour or wrongdoings are at all times assessed by the hotline. The assessment could result in an investigation. This Regulation explains:

- How reports will be assessed;
 - When an investigation will be launched;
 - How the investigation will be conducted;
- If, how and what sanctions will be imposed is set out in the Regulation on sanctions.

4.2 Initial assessment of the report

All reports are taken seriously. This does not mean that all reports will automatically lead to an investigation. The hotline makes an initial assessment of the report. The assessment is based on the following criteria:

- The nature of the report
 - Is this something which can be reported via the Regulation
 - on reporting apparent or suspected wrongdoings, violations of integrity and undesirable behaviour?
 - What type of wrongdoing, integrity violation or undesirable behaviour does the report relate to?
 - Could this possibly be a criminal offence?
 - Are there external authorities or inspectorates that could play a role in this?
- Admissibility
 - Is this report eligible to be dealt with?
 - Is the AFM authorised to investigate the report?
 - Are there more appropriate procedures for the reported issue, such as the disciplinary law of certain professions?

- The severity
 - The severity of the issue can be determined based on: The fact itself
 - The context in which the fact took place
 - The individual or the individual's position to whom the report relates
 - Possible danger, social or political sensitivity.
- Verifiability
 - Are there sufficient leads to start a possible investigation?
 - Is there adequate information available?
 - Is there additional information available?
 - Are there appropriate means to investigate the report?
- The reporting individual's position
 - How much insight did the reporting individual actually have in the suspected wrongdoing,
 - integrity violation or undesirable behaviour?
 - How much knowledge does the reporting individual have?
 - Is the reporting individual able to provide more information?
 - How reliable is the report?
- Position of the individual involved
 - Who committed the suspected wrongdoing, integrity violation or undesirable behaviour?
- Credibility/probability
 - What is the link between the information from the report and the facts and circumstances as known to the organisation?
 - Is it possible that the suspected wrongdoing, integrity violation or undesirable behaviour has taken place?
 - Is it possible to rule out the suspected wrongdoing, integrity violation or undesirable behaviour with certainty?

Antecedents can also be the subject of a report. As stated in the AFM Code of Conduct, all employed AFM employees must disclose their antecedents. If the antecedent raises any questions about that

person's reliability, the report may prompt an in-house screening and further investigation. In-employment screening and the assessment of antecedents are set out in the Screening Regulation.

The initial assessment of the report will lead to a decision as to whether the report will be investigated. The hotline advises the competent authority. The decision is taken by the competent authority. The competent authority in question depends on the type of report. See the Regulation on reporting apparent or suspected wrongdoings, violations of integrity and undesirable behaviour.

The hotline may also receive signals for which no official report was made. If such signals indicate apparent or suspected wrongdoings, integrity violations and/or undesirable behaviour, it may prompt an investigation. The decision to launch an investigation is taken by the competent authority. See the Regulation on reporting apparent and suspected wrongdoings, violations of integrity and undesirable behaviour.

For more information on the reporting procedure see the Regulation on reporting apparent or suspected wrongdoings, violations of integrity and undesirable behaviour.

4.3 Follow-up steps

Different follow-up steps may be taken depending on the assessment of the report:

1. *No investigation*, the report will not be investigated further and the file will be closed
2. *An investigation is launched*

Actions in the decision to launch an investigation

Before initiating an investigation, consideration is made of the following actions:

- Action: securing data
 - The investigative team ensures that data are secured. The Data Protection Officer will be involved in this if needed. This also includes securing company resources. Securing data is something which can also be done during the investigation.

- Action: consideration whether to impose a suspension
 - If an investigation is launched, it could be a consideration to suspend the employee. This will only be done in exceptional circumstances such as criminal offences, including fraud and economic criminal offences. The investigative team will propose such a suspension. The decision to do so is taken at the level of the Executive Board, in consultation with the head of HR & FB. In some cases, the opposite could apply, where it is imperative for the person involved to stay in office. The timing of a suspension depends on the facts and circumstances. The suspension can also take place during the investigation.
- Action: communication
 - The investigators decide who is informed about what. The starting point is that the circle of informed individuals should be as small as possible. It requires diligence and necessity. If needed, a communication plan is drawn up, describing for each internal or external stakeholder who will be informed about what and when.

4.4 Investigation procedure

Investigations are carried out by an independent investigative team consisting of at least two persons. Depending on the report, the investigative team will be assembled from among the members of the hotline, joined by the general counsel if applicable, i.e. in cases where the report refers to undesirable behaviour, and/or colleagues from the Computerisation Division, the team handling online research or the IAD. The investigative team can also be joined by external parties or be outsourced externally. See the Regulation on reporting apparent or suspected wrongdoing, violations of integrity and undesirable behaviour. The investigative team is given the instruction to conduct an investigation or further investigation into the facts. The decision to launch an investigation is taken by the competent authority. See the Regulation on reporting apparent or suspected wrongdoing, violations of integrity and undesirable behaviour.

The investigation can consist of a **regular investigation** or a **special investigation**. Serious violations can take the form of a special investigation. Serious violations are in any case understood to mean criminal offences and apparent or suspected wrongdoings. In cases of a serious violation, the investigative team may also conclude that

they need to report this to the Public Prosecution Service or that they have to inform other authorities, such as the Fiscal Intelligence and Investigation Service (FIOD), the Dutch DPA or an inspectorate. The investigative team will communicate this recommendation to the chair of the Executive Board or, if the case involves a member of the Executive Board, the chair of the Supervisory Board, either of whom will then make a decision. If the investigation concerns the chair of the Supervisory Board, the investigative team will report directly to the vice chair of the Supervisory Board.

Guiding principles of the investigation

The following guiding principles apply for launching an investigation:

- Data will be collected lawfully and proportionally;
- Data that have been obtained unlawfully will not be used;
- The principles of Dutch and European privacy laws and regulations will be applied;
- Both sides will be given the opportunity to present their case. If not during the investigation, this opportunity will be provided at the latest before the decision is made about the investigation.

Investigation methods

There are various investigation methods. Starting principles when choosing a method of investigation are proportionality and subsidiarity. The investigation into the facts has to be proportional and match the nature and severity of the report. The least invasive investigation method must be deployed to achieve the goal, i.e. subsidiarity.

Relevant information

The members of the investigative team are allowed to inspect and request all documents of the AFM, i.e. all relevant documents, which they reasonably consider necessary for their investigation.

Regular investigation

Regular investigation involves a document review and interviews with the individuals concerned. The investigative team will at all times give the reporting individual the opportunity to explain the report in an interview and to substantiate the facts. The investigative team can also

invite other individuals for an interview, including those individuals who are subject of the report. The investigative team ensures that each interview will be recorded in writing. This record will be submitted for review, correction, approval and signature to the individual interviewed.

If it transpires during the investigation that the report is unfounded, the investigation will be discontinued. The hotline informs the reporting individual and the individual concerned. If the outcome is established, this may result in a mitigating measure or sanction.

Special investigation

As well as using the investigation methods from the regular investigation procedure, the investigative team can also employ alternative approaches. This could include a search of the physical work environment and company resources used, or commissioning such a search, or observations techniques and the use of cameras. Permission for the deployment of these investigation methods is given by the chair of the Executive Board. If the investigation concerns the chair of the Executive Board or a member of the Supervisory Board, the chair of the Supervisory Board will give permission for such deployment. If the investigation concerns the chair of the Supervisory Board, the vice chair of the Supervisory Board will give this permission.

4.5 Notification to the individual involved at the start of the investigation

The individuals who are the subject of the report will be notified by the investigators as soon as the investigation begins. This will in any event be once a decision to proceed with an investigation has been made, unless there is a serious risk that such notification compromises effective investigation into the report by the AFM. The individual involved must in any event receive notification as soon as this risk no longer applies.

The individuals involved will be notified about:

- the facts they have been accused of
- those persons having received the notification

- the fact that the AFM is responsible for the Regulation
- the ways in which the individuals involved can exercise their rights to access, rectification, erasure, or restriction of their personal data.

The individual involved will not receive any information about the identity of the individual who made the report.

4.6 Draft report

The investigative team draws up a draft report. The team gives the reporting individual and those individuals who are the subject of the report the opportunity to respond to this, unless serious objections are raised against it. Those responses will be included in the report.

4.7 Decision and consequences

The investigative team will submit an investigation report. The compliance officer will receive a copy of the report and will give recommendations on possible sanctions and/or mitigating measures. Mitigating measures may include a policy adjustment or the reinforcement of control measures. In the case of a sanction, this will be imposed in the manner as described in the Regulation on sanctions. The reporting individual and those concerned will receive a written statement of the main results from the investigation, unless serious objections are raised against this.

4.8 Secrecy and confidentiality

All those involved in a report have a duty to maintain confidentiality with regard to the information, unless they are legally bound to disclose this. In addition to the above, information regarding the report will only be made available to those parties within the AFM who need this knowledge to allow them to fulfil their duties in connection with this Regulation, including duties such as investigation and the follow-up of the investigation. These persons, too, have a duty to maintain confidentiality.

Confidential data are in any case understood to include the identity of the reporting person and the accused persons and information that

can be traced back to them, as well as information relating to trade secrets. The reporting individual's identity is only known to the hotline, as indicated above.

Also see the Regulation on reporting apparent or suspected wrongdoing, violations of integrity and undesirable behaviour.

Delegation of duties

Within the AFM, the following officials are involved in and responsible for the assessment and follow-up of the reports and for the investigation to be conducted:

Hotline

- Assessing the report (triage)
- Monitoring the progress and deadlines of the reporting procedure and the investigation procedure.
- Liaising with the reporting individual

Investigators

- Listing the facts independently. Investigators
- can be appointed/hired in-house or externally

General counsel

- May join the investigative team if the report relates to undesirable behaviour.

The Regulation on reporting apparent or suspected wrongdoing, violations of integrity and undesirable behaviour states who takes the decision to launch an investigation.

File management

The hotline and the investigative team document their work and record and store all information provided by employees or third parties in a separate confidential file. The investigation report does not form part of either the concerned employee's personnel file or the reporting individual's personnel file. The investigations conducted and actions taken will be archived in a secure environment.

Privacy

The hotline and the investigative team will treat any data and information received in connection with this Regulation as confidential at all times. Personal data processing in connection with the provisions

in this Regulation will be carried out in accordance with the guidance provided in the General Data Protection Regulation (GDPR) and other applicable laws and regulations, and will be retained in accordance with the AFM data retention policy. More information on employees' privacy rights according to the GDPR are included in the in-house privacy regulations for AFM employees.

Residual powers

In all cases not provided for in this Regulation with respect to employees other than members of the Executive Board, a member of the Executive Board is empowered to adjudicate, issue instructions and take certain measures. With respect to members of the Executive Board or Supervisory Board, this authority rests with the chair of the Supervisory Board or, if the case concerns the chair of the Supervisory Board, the vice chair of the Supervisory Board.

Complaints procedure

If the reporting individual or another concerned party disagrees with the manner in which the Regulation has been implemented, they may submit a complaint to the AFM Complaints Committee. For further details, please refer to the AFM Complaints Procedure.

Entry into force

This Regulation was revised in a number of respects and will enter into force on 1 May 2025.

Approval

This Regulation is adopted by the Executive Board and approved by the Supervisory Board, following the Works Council's consent, if required.

Review and update

This Regulation is maintained and reviewed by the CIR manager, and revised, where needed. The review takes place once every three years or more often if warranted. Any material change passes to the Executive Board and Supervisory Board and is communicated to the AFM employees.

Exceptions/deviations from the Regulation

All requests to deviate from the Regulation must be submitted to the owner, i.e. the CIR manager. Deviations from this Regulation will be recorded in writing, stating reasons.

5. The regulation on sanctions

5.1 Introduction

Acting in violation of the Code of Conduct and/or the regulations from the Integrity Policy can be deemed a serious breach of the trust that the AFM must be able to have in its employees, and on that basis can lead to one or more appropriate sanctions.

This Regulation aims to provide guidelines for imposing sanctions in those cases where the Code of Conduct and/or associated regulations in the Integrity Policy have been violated. Violations include antecedents, breaching the Regulation on private investment transactions, undesirable behaviour, violations of in-house policy, and wrongdoings.

This Regulation relates to violations. It may be that an investigation is required before deciding on a sanction, i.e. an investigation as referred to in the Regulation on integrity investigation. No sanctions may be imposed in anticipation of the results of the investigation, except in the event of a disciplinary measure as referred to in the Regulation on integrity investigation.

5.2 Framework for assessing sanctions

If the investigation confirms that a violation has taken place, the compliance officer will make a recommendation on whether a sanction should be imposed and if so, which one. When deciding this, the compliance officer will review whether the violation is a minor or a serious violation.

The assessment of the violation is based on the following weighting factors:

- a. **Severity:** is this a violation that would impair the integrity with which the employee can fulfil and perform their role? Does it involve a minor or serious violation?

In this regard, it is also relevant whether the incident has any impact on society or the AFM.

There are minor and serious violations. For example:

Minor violation

- An employee forgets to disclose the investment component of the mortgage when purchasing a home.
- However, if it is also found that the employee used inside information when setting up the investment component of this mortgage, the same offence will be classified as a serious violation.
- Failure to timely disclose investment accounts.
- Violations of general rules of conduct are also deemed to be minor violations.

Serious violation

- Repeat offences, of minor or serious offences.
- Insider trading.
- Leaking confidential supervisory information.
- Theft.
- Abuse of powers granted based on an individual's position and/or duties.
- Economic offences such as tax fraud, forgery, corruption and bribery.
- Incidents that jeopardise the interests of society, because there is danger to health, for example, or danger to the safety of persons or other wrongdoings.
- Intimidation.
- Discrimination.
- Aggression and violence.
- Bullying.
- Sexual harassment.

- b. **Culpability:** Among other things, assessing culpability means reviewing the extent to which the employee has acted unlawfully or was aware or should have been aware of the unlawfulness of the acts, and what their intentions were when they acted. This includes but is not limited to the following:
 - *Whether the acts were intentional or not:* Was the individual's

act and/or failure to act deliberate and what intentions did they have? How was the matter viewed at the time the violation was perpetrated?

- *Capacity*: Was the individual acting in a private or work-related capacity when they committed the violation? What role or position does the individual hold?
- Has inside information or confidential supervisory information been used?
- *Is this a repeat offence?*: Has the employee previously committed similar violations? Are there previous occasions on which an instructive interview was held or a warning was given?
- *Duration of the violation*: It is important to establish when the violation began and ended. Did the employee cease the illegal behaviour as soon as they became aware that they were committing a violation? A violation that has continued for an extended period of time will weigh more heavily than a one-off violation.

c. **Reporting, attitude and ability to learn**: The extent to which the employee demonstrates transparency will carry significant weight in the assessment. Was the report made by the employee themselves or not? Consideration will also be given to the attitude adopted by the employee during the investigation. The employee's attitude, motives and clarification show whether the employee too considers their actions and/or failure to act to be serious, whether they understand the incident should not have taken place and whether they have learnt from it.

d. **Combination**: Has the employee been involved in incidents more frequently, whether in a culpable manner or otherwise? Once the severity and culpability have been established, the decision as to what sanction should be imposed will also take account of the following principles:

- *Proportionality*: The measure must be proportionate to the violation;
- *Consistency*: The actions taken must be in line with those taken in similar cases in the past;
- *Exceptional circumstances*: All facts and circumstances must be

taken into account, including both mitigating and aggravating circumstances.

Mitigating circumstances include a good record of service, approval of the action by a line manager, a long record of service, failure by a line manager to challenge or adequately challenge the employee, is there any exertion of influence or even inducement from the AFM, or inadequacies in the process and controls within the organisational unit.

Aggravating circumstances may include previous warnings by the line manager, serious damage to interest and credibility of the AFM, an exemplary role owing to the individual's position, abuse of specific position-related powers, personal financial gain, previously imposed sanctions or repeat behaviour.

5.3 Examples of sanctions

The nature of the offence will determine what sanction is imposed. No indication can be given as to what sanction will be attached to which violation. This must be assessed on a case-by-case basis, considering the specific circumstances that apply, such as the nature and severity of the violation, as well as the employee's personal circumstances. Below is a non-exhaustive overview of possible sanctions.

Minor sanctions

- Entry in the compliance file and/or an instructive conversation on compliance with standards.
- Mandatory reversal of the private transaction executed, with any additional proceeds being donated to charity.
- Following a training course or discussing the incident in a work meeting.

Severe sanctions

- Written reprimand or a warning
- Suspension or compulsory leave of absence
- Discontinuation or withholding of wages
- Invoking the contractual penalty clause
- Withdrawal of facilities

- Recovery of losses from the employee
- Reassignment to a different division
- Reassignment to a different, potentially lower position
- Start-up of an exit procedure
- Dismissal with immediate effect

In the event that a violation qualifies as a criminal offence, the Executive Board or, if a member of the Executive Board is involved, the chair of the Supervisory Board, or, if the chair of the Supervisory Board is involved, the vice chair of the Supervisory Board, may decide to notify the competent authorities in criminal matters or to notify other authorities. The Minister of Finance is authorised to suspend or terminate the employment of the members of the Executive Board and the members of the Supervisory Board.

5.4 Decisions and imposing sanctions

The compliance officer will prepare a recommendation as to whether a sanction should be imposed or not. The compliance officer will do so as soon as an investigation has clarified the facts and circumstances of the violation.

Who will then decide whether a sanction should be imposed or not? The compliance officer will submit recommendations involving minor sanctions to the CIR manager, who will use the recommendation issued by the compliance officer to determine whether a sanction should be imposed. The employee will be given the opportunity to express their views to CIR on the proposed decision on a sanction to be imposed. The CIR manager imposes the sanction.

Recommendations involving a **severe sanction** will be coordinated with the CIR manager, the head of HR & FB and, if appropriate, the general counsel, after which the compliance officer will submit them to the Director of Operations. Based on CIR's recommendation, the Director of Operations decides whether and if so, which sanction is to be imposed. The employee will be given the opportunity to express their views to the Director of Operations on the proposed decision on a sanction to be imposed. The sanction will be imposed by the Director of Operations.

For cases involving a member of the Executive Board or the Supervisory Board, the recommendation will be coordinated with the chair of the Supervisory Board. The chair of the Supervisory Board takes the decision and imposes the sanction. For cases involving the chair of the Supervisory Board, the vice chair of the Supervisory Board will be authorised to impose a sanction. In cases that involve a CIR employee or CIR manager, the general counsel makes a recommendation for the chair of the Executive Board. The chair of the Executive Board imposes the sanction.

5.5 Option to appeal

Following the imposition of a severe sanction, employees may lodge a written appeal with the chair of the Executive Board. The appeal must be lodged within four weeks of the sanction having been imposed. Appeals in respect of a minor sanction can be lodged with the Director of Operations. Employees must substantiate why they disagree with the sanction that has been imposed. The employee will send this to the secretary of the Executive Board, who will then pass this to the officer responsible for reviewing the appeal. The appeal does not allow for a more severe sanction to be imposed on the employee. The Director of Operations or the chair of the Executive Board will issue a decision within four weeks of this date.

After the appeal procedure, the employee can also decide to launch legal proceedings in order to seek termination of the measure.

Delegation of duties

Within the AFM, the following officials are involved in and responsible for giving recommendations, deciding and imposing sanctions.

Compliance officer

- Gives recommendations to the CIR manager about whether or not to impose minor sanctions.

Gives recommendations involving severe sanctions to the Director of Operations, in coordination with the CIR manager, the head of HR & FB and the general counsel, if applicable.

- Gives recommendations involving minor or severe sanctions to the chair of the Supervisory Board if the violation involves a member of the Executive Board or a member of the Supervisory Board.

- Gives recommendations involving minor or severe sanctions based on the decision framework to the vice chair of the Supervisory Board if the violation involves the chair of the Supervisory Board.
- Records minor sanctions imposed in the compliance file.

CIR Manager

Takes the decision on whether or not to impose a minor sanction.

General counsel

- Gives recommendations involving minor or severe sanctions if the violation involves a CIR employee or CIR manager.

Executive Board

- Is authorised to file a report with the competent criminal authorities or to notify other authorities.

Chair of the Executive Board

- Makes the decision on whether or not to impose minor sanctions or severe sanctions if the violations involve a CIR employee or CIR manager and imposes these sanctions.
- Decides on appeals against severe sanctions.

Director of Operations

- Makes the decision on whether or not to impose severe sanctions.
- Imposes severe sanctions.
- Decides on appeals against minor sanctions.

Secretary of the Executive Board

- Forwards the written appeals against minor or severe sanctions to the Director of Operations and the chair of the Executive Board.
- Informs the employee about the findings of the appeal.

Chair of the Supervisory Board

- Makes the decision whether or not to impose minor sanctions or severe sanctions if the violation involves a member of the Executive Board or member of the Supervisory Board.

- Imposes minor sanctions or severe sanctions if the violation involves a member of the Executive Board or member of the Supervisory Board.

Vice chair of the Supervisory Board

- Makes the decision whether or not to impose minor sanctions or severe sanctions if the violation involves the chair of the Supervisory Board.
- Imposes minor sanctions or severe sanctions if the violation involves the chair of the Supervisory Board.

HR & FB

- Records severe sanctions imposed in the personnel file.

File management

Minor sanctions that are imposed will be documented in the compliance file, whereas severe sanctions will be documented in the employee's personnel file by HR & FB. This will be done once the employee has been informed. Only the compliance officer is able to access the compliance file. The personnel file is maintained by HR & FB. The information stored in the personnel file could have consequences for employees who apply for a position with another employer, should this employer conduct a reference check and request an integrity statement from the AFM.

Privacy

The compliance officer and the HR & FB division will treat any data and information received in connection with this Regulation as confidential at all times. Personal data processing in connection with the provisions in this Regulation will be carried out in accordance with the guidance provided in the General Data Protection Regulation (GDPR) and other applicable laws and regulations, and will be retained in accordance with the AFM data retention policy. More information on employees' privacy rights according to the GDPR are included in the in-house privacy regulations for AFM employees.

Residual powers

In all cases not provided for in this Regulation with respect to employees other than members of the Executive Board, a member of the Executive Board is empowered to adjudicate, issue instructions and take certain measures. With respect to members of the Executive Board or members of the Supervisory Board, this authority rests with the chair of the Supervisory Board or, if the case concerns the chair of the Supervisory Board, the vice chair of the Supervisory Board.

Complaints procedure

If the reporting individual or another concerned party disagrees with the manner in which the Regulation has been implemented, they may submit a complaint to the AFM Complaints Committee. For further details, please refer to the AFM Complaints Procedure.

Entry into force

This Regulation was revised in a number of respects and will enter into force on 1 May 2025.

Approval

This Regulation is adopted by the Executive Board and approved by the Supervisory Board, following the Works Council's consent, if required.

Review and update

This Regulation is maintained and reviewed by the CIR manager, and revised, where needed. The review takes place once every three years or more often if warranted. Any material change passes to the Executive Board and Supervisory Board for approval and is communicated to the AFM employees.

Exceptions/deviations from the Regulation

All requests to deviate from the Regulation must be submitted to the owner, i.e. the CIR manager. Deviations from this Regulation will be recorded in writing, stating reasons.

6. The regulation on complaints of undesirable behaviour

6.1 Introduction

Together, we create a safe and healthy working environment. The AFM does not tolerate undesirable behaviour and aims to protect its employees from this. The AFM Code of Code describes what is considered undesirable behaviour at the AFM.

Should employees unexpectedly encounter undesirable behaviour, the preferred approach is to first attempt to address and resolve the undesirable behaviour with the offending party. Employees can also turn to their line manager, HR & FB or one of the confidential counsellors. If those attempts are unsuccessful, or if the nature of the conduct and/or relationship is such that raising the issue is not an option, the employee can submit a report to the hotline.

The hotline assesses the report as described in the Regulation on integrity investigation. Possible solutions may include a meeting or a corrective interview, mediation, submitting a complaint or initiating an internal investigation. If the employee chooses to file a complaint, the hotline will pass on the complaint to the chair of the Complaints Committee for undesirable behaviour (Complaints Committee). A complaint can be dramatic and confrontational for all parties involved, and thus requires great care. This Regulation explains the proceedings of a formal complaint of undesirable behaviour. An internal investigation is conducted as described in the Regulation on integrity investigation.

The stakes are high when it comes to complaints about undesirable behaviour. If the complaint proves to be well-founded, it may result in serious repercussions for the individual involved. That said, if the complaint is deemed unfounded, this outcome might be equally distressing for the complainant. A fair and thorough process is essential to safeguard the interests of both the complainant and the accused. This means that the Complaints Committee has to be objective in handling the complaint. This committee is able to form an

independent opinion and has no interests in the outcome.

Based on an investigation into the complaint, the Complaints Committee will issue an opinion on the plausibility of the complaint and can ultimately decide to impose an employment or other measure. It is both a commitment and requirement for the AFM to act as a good employer and as such the AFM attaches great value to the proper handling of complaints.

6.2 Complaints Committee for undesirable behaviour

The AFM has established a special Complaints Committee that will review complaints in accordance with this Regulation. The AFM will provide the Complaints Committee with the facilities it reasonably requires for the performance of the duties it has been tasked with.

The Complaints Committee consists of the general counsel and a compliance officer as a minimum. The general counsel may invite other employees to participate in the committee, if additional expertise is required, for example. Those additional members are appointed by the Executive Board. The role of chair of the Complaints Committee will be fulfilled by the general counsel. In the event that one of the members is unable to participate, the chair of the Executive Board is authorised to appoint one or more other employees to the committee. The primary consideration for this appointment will be the independent position of these individuals.

Members of the Complaints Committee must withdraw in the event that they are involved in the complaint or any circumstances surrounding it, as well as in the event that an actual or apparent conflict of interests arises. In such cases, the chair of the Executive

Board will appoint another employee to the committee.

The Complaints Committee will be supported by a secretary to be appointed by the Executive Board. The remit of the secretary will be elaborated further by the Complaints Committee.

It is the responsibility of the Complaints Committee to:

- a. Investigate complaints submitted to the Complaints Committee
- b. Provide a written opinion stating reasons to the chair of the Executive Board on whether the allegations made by the complainant appear plausible;
- c. Provide a written opinion stating reasons to the chair of the Executive Board on any measure to be imposed. If this measure is an employment measure, the advice of the head of HR & FB must be sought.

During the investigation, the chair of the Executive Board, having consulted the Complaints Committee, may decide to take temporary employment measures and/or launch a regular or special investigation. In case of the latter, the chair of the Executive Board may decide to suspend the time limit referred to in 6.6 of this Regulation.

6.3 Submitting a complaint

If the employee has opted to lodge a complaint, the hotline will pass on the complaint to the chair of the Complaints Committee.

The complaint must comprise:

- a. The name of the complainant;
- b. A description of the behaviour that is the subject of the complaint and the period over which said behaviour has taken place or is taking place;
- c. The name of the accused person or persons and, if applicable, any witnesses;
- d. A description of the steps the complainant has already taken and any written documents pertaining to these;
- e. The date and the complainant's signature.

The Complaints Committee may request the complainant to verbally explain the complaint.

6.4 Consideration of a complaint

Within seven calendar days of having received a complaint, the Complaints Committee will send the complainant written confirmation of receipt and a copy of this complaints procedure. The confirmation will state the date on which the complaint was received.

The Complaints Committee must inform the complainant within twelve calendar days of receipt whether their complaint is admissible. The Complaints Committee is not under any obligation to consider a complaint if:

- a. The complaint does not pertain to undesirable behaviour as described in the AFM Code of Conduct;
- b. The complaint has been submitted on behalf of others;
- c. The complaint has been made anonymously;
- d. The Complaints Committee is of the opinion that, following a request for further information, the complainant has not adequately enabled the committee to take cognizance of relevant information necessary in order to consider the complaint;
- e. The Complaints Committee has considered the complaint previously, unless there are new facts or circumstances;
- f. The behaviour which is the subject of the complaint dates back more than one year, unless there are new facts or circumstances;
- g. The behaviour is the subject of legal proceedings, whether ongoing or concluded;
- h. The behaviour which is the subject of the complaint is being investigated or prosecuted by the police or judicial authorities.

In the event the complaint is declared admissible, a notification will be sent to the complainant, the accused and the Executive Board. In the event the complaint is declared admissible, the accused will receive a copy of the complaint. The accused will be given the opportunity to put forward a defence to the Complaints Committee within twelve calendar days of receipt of the copy. The defence must be sent to the chair of the Complaints Committee.

Within seven calendar days of having received the defence, the Complaints Committee will provide a copy thereof to the complainant for information.

6.5 Complaints handling – Investigation and hearing

If the Complaints Committee decides to declare the complaint admissible, it will begin a substantive examination.

The Complaints Committee will carefully examine whether a complaint is founded. To this end, the Complaints Committee will hear the complainant and the accused, and have the option to consult other internal or external individuals, witnesses and/or experts, whether or not on the basis of information provided by the complainant or the accused. The Complaints Committee will be able to hear individuals on multiple occasions.

The complainant and the accused will be heard at separate hearings, unless both the complainant and the accused declare that they have no objection to a joint hearing.

The Complaints Committee will have access to documents, systems and individuals as needed in order to arrive to an opinion. The relevant individuals will be obliged to lend their cooperation and appear at any hearing that is held. The time required for this purpose will be considered working time.

Each hearing will be attended by no less than two members of the Complaints Committee. The Complaints Committee will prepare minutes for each hearing, which the individual heard must sign for approval, with or without comments, within a reasonable time limit to be set by the committee. If the person heard refuses to sign, this will be noted in the report, stating the reasons. If there is no response within the time limit set by the Complaints Committee, this will be taken as tacit approval.

In the interest of ensuring the records are as complete as possible, an audio recording may be made during the hearing, provided the individuals to be heard have agreed to this. This audio recording is for supplementary purposes only and will not replace the written report of the hearing.

The complainant and the accused may respond within seven calendar days to the documents drawn up for the Complaints Committee.

The complainant and the accused may ask an adviser internal or external to the AFM to support them during the hearings. The AFM may reimburse the cost of an adviser up to a reasonable amount.

6.6 Recommendation by the Complaints Committee

No later than six weeks after receipt of a complaint, the Complaints Committee will communicate a substantiated written report to the chair of the Executive Board, in accordance with the provisions of 6.5. The report sets out the committee's recommendation on the admissibility of the complaint.

In the event that it is not possible to complete the recommendation within the specified time limit, the Complaints Committee is able to extend the time limit by a maximum of four weeks. The Complaints Committee will communicate such extensions to the complainant, the accused and the chair of the Executive Board in writing. Further extension will be possible if the complainant agrees to this in writing.

6.7 Decision by the chair of the Executive Board

The chair of the Executive Board makes a decision about the complaint. Within twelve calendar days of receipt of the Complaints Committee's recommendation, the chair of the Executive Board will use the recommendation issued by the Complaints Committee to rule on the complaint. If the chair of the Executive Board deems the complaint plausible, the complaint will be upheld and the chair may then decide to impose a measure. If this measure is an employment measure, the advice of the head of HR & FB must be sought.

In the event that the chair of the Executive Board decides not to follow the recommendation of the Complaints Committee, the chair will set out the arguments for this in the decision. The intention to deviate from the recommendation must be discussed with the Complaints

Committee before any decision to do so. In this event, the time limit specified under a in the first paragraph will be extended by twelve calendar days.

If an employment measure is imposed, the accused will be entitled to provide a response to this. This response must be submitted within twelve calendar days from the announcement of the intended decision by the Executive Board. The assessment of the accused's response will include a request to the Head of HR & FB for advice.

The decision taken by the chair of the Executive Board, including the recommendation by the Complaints Committee and the hearing reports, will be notified to the Complaints Committee, the complainant and the accused in writing.

The chair of the Executive Board may decide to consult the other members of the Executive Board on an anonymous basis with regard to the recommendation and the measures to be taken.

At the request of the complainant and/or the Complaints Committee, the chair of the Executive Board may put in place temporary measures both before and during the handling of the complaints, if this is necessary in the interest of the complainant's well-being and/or the circumstances are deemed untenable for one or more of the directly concerned parties.

The complainant is able to withdraw the complaint up until the time the Complaints Committee issues its recommendation to the chair of the Executive Board. Withdrawal must be effected by means of a written notification to the Complaints Committee. In the event of a withdrawal, the Complaints Committee will ensure the file is destroyed.

6.8 Confidentiality

Anyone involved in the handling of a complaint on the basis of this Regulation will be subject to a duty of confidentiality, unless a statutory obligation to disclose applies. The duty to maintain confidentiality does not apply if the complainant or the accused wants to seek help from someone who is bound by a duty of confidentiality because of their office or profession. This obligation also lapses if the individual wants to file a report of possible criminal offences relating to the complaint.

6.9 Legal protection

There is no possibility to object or appeal against decisions taken by the chair of the Executive Board on the basis of this Regulation.

Unless a legal right is found to have been abused, the complainant and any witnesses may not suffer any disadvantage in relation to their legal position as a result of the submission of a complaint or their role or actions under this Regulation.

Accused individuals will also have their legal position protected. This means the accused will be deemed innocent until proven otherwise.

The members of the Complaints Committee cannot be held liable for recommendations made by the Complaints Committee or any act of failure to act in their capacity as members of the Complaints Committee.

6.10 Registration and reporting

The accused will only have the measure imposed and the reasons for this recorded in their personnel file. The accused will be informed of this in writing. The information required for this will be provided to the Head of HR & FB by the Complaints Committee.

The hotline records the complaint in the reports register and draws up an annual report about wrongdoings, integrity violations and complaints. The chair of the Executive Board receives this report, at the same time as the Works Council.

6.11 Supervisory Board

Where a complaint relates to conduct by a member of the Executive Board or a member of the Supervisory Board, the tasks and powers set out in this Regulation for the chair of the Executive Board will be taken over by the chair of the Supervisory Board. Where a complaint relates to conduct by the chair of the Supervisory Board, the tasks and powers set out in this Regulation will be taken over by the vice chair of the Supervisory Board.

Privacy

The Complaints Committee will treat any data and information received in connection with this Regulation as confidential at all times. Personal data processing in connection with the provisions in this Regulation will be carried out in accordance with the guidance provided in the General Data Protection Regulation (GDPR) and other applicable laws and regulations, and will be retained in accordance with the AFM data retention policy. More information on employees' privacy rights according to the GDPR are included in the in-house privacy regulations for AFM employees.

Residual powers

In all cases not provided for in this Regulation with respect to employees other than members of the Executive Board, a member of the Executive Board is empowered to adjudicate, issue instructions and take certain measures. With respect to members of the Executive

Board or members of the Supervisory Board, this authority rests with the chair of the Supervisory Board or, if the case concerns the chair of the Supervisory Board, the vice chair of the Supervisory Board.

Entry into force of this Regulation

This Regulation was revised in a number of respects and will enter into force on 1 May 2025.

Approval

This Regulation is adopted by the Executive Board and approved by the Supervisory Board, following the Works Council's consent, if required.

Review and update

This Regulation is maintained and reviewed by the CIR manager, and revised, where needed. The review takes place once every three years or more often if warranted. Any material change passes to the Executive Board and Supervisory Board for approval and is communicated to the AFM employees.

Exceptions/deviations from the Regulation

All requests to deviate from the Regulation must be submitted to the owner, i.e. the CIR manager. Deviations from this Regulation will be recorded in writing, stating reasons.

Definitions and explanatory notes

In the Code of Conduct and the Integrity Policy the following shall be taken to mean:

Activity:

An ancillary position or ancillary activity which the employee currently undertakes, has undertaken or wishes to undertake during or after their duties for the AFM. Excluded from this are activities arising from the responsibilities or work of the AFM, which employees perform by virtue of their role or exclusively perform by virtue of their role with the AFM.

Anonymous reporting:

A report made without the reporting individual disclosing their identity.

Antecedent:

A violation or integrity violation that has resulted in the imposition of a measure and/or sanction. In screenings for employees, a distinction is made between three categories of antecedents:

- Criminal antecedents
- Supervisory antecedents (applicable only to vulnerable positions)
- Other antecedents, including conflicts in the workplace and/or disciplinary measures.

Accused:

The individual against whom a complaint has been made.

Conflict of interest:

- This arises when an employee has a personal interest or
- a role-based interest (conflict of duty) as a result of ancillary or other positions or duties,
- and should therefore be deemed incapable of safeguarding the interest of the AFM with integrity and free from prejudice.

Investment:

The execution of private investment transactions for the purpose of acquiring or disposing of financial instruments. See the definition of financial instruments, or arranging for the execution thereof.

Collective investment scheme:

A unit trust, investment company or undertaking for collective investment in transferable securities (abbreviation: ICBE) as referred to in Section 1(1) of the Financial Supervision Act.

Detriment:

Detriment refers to the deliberate disadvantaging of an individual. Examples of detriment in any event include dismissal or suspension, a fine as referred to in Article 7:650 of the Dutch Civil Code, demotion, withholding promotion, a negative performance review, a written reprimand, discrimination, intimidation, bullying or exclusion, slander or defamation, early termination of an agreement to provide goods or services, and withdrawal of a licence.

The prohibition of detriment means that reporting individuals may not be disadvantaged during and after the handling of a report or public disclosure of a suspicion of wrongdoing. The aforementioned legal protection is subject to the condition that the reporting individual has reasonable grounds to believe that the information regarding the report is accurate at the time of reporting. This protection also applies to advisers, the hotline, the investigators and any third parties involved.

Involved third party:

- a third party connected to you as a reporting individual who may be disadvantaged by the AFM or a person or organisation to whom or which you as a reporting individual are otherwise connected in a work-related context, and
- a legal entity owned by you as a reporting individual, for which you as a reporting individual work or to which you as a reporting individual are otherwise connected in a work-related context.

Competent authorities:

Competent authorities as referred to in the Whistleblowers Protection Act are understood to mean:

- The Netherlands Authority for Consumers and Markets.
- The Dutch Data Protection Authority.
- The Dutch Central Bank (De Nederlandsche Bank, DNB).
- The Dutch Whistleblowers Authority (Huis voor Klokkenluiders).
- The Dutch Health and Youth Care Inspectorate.
- Dutch Healthcare Authority.
- The Authority for Nuclear Safety and Radiation Protection.
- Organisations and administrative bodies, or parts thereof, designated by general administrative order or ministerial regulation, that have duties or powers in one of the areas referred to in Article 2(1) of Directive (EU) 2019/1937.
- An administrative body, a service or other competent authority, not being a competent authority as mentioned above, which by virtue of a duty or power assigned by law, pursuant to the law or in mandate, receives a report of a breach of Union law.

They may receive reports and investigate them or take measures based on a report of breach of the law and the law of the European Union (Union law).

UCITS (Undertaking for Collective Investment in Transferable Securities):

A fund or company as referred to in Section 1(1) of the Financial Supervision Act.

Rights issue:

A rights issue is an issue which gives existing shareholders preferential rights over new shareholders when subscribing to the rights issue.

Compliance file:

All employees have a compliance file. The file contains all the information provided by the employee regarding ancillary activities, private investments, disclosed gifts and, where applicable, any comments made by the compliance officer. The file can only be accessed by compliance officers and the relevant employee.

Compliance officer:

An employee in the Compliance, Integrity & Risk Management (CIR) division tasked with the internal supervision of compliance with the Code of Conduct and the Integrity Policy.

Crypto-assets:

A digital representation of a value or right that can be traded via a distributed ledger, such as a block chain, or similar technology.

Crowdfunding:

Crowdfunding is defined as the practice of investing with, or lending of funds from a large group of investors to companies or consumers (project owners) using publicly-accessible online platforms, i.e. crowdfunding platforms.

Data Breach:

A data breach is understood to mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data.

Dilemma:

This always means a conflict between different values. For that reason, there is no 'right' answer in a dilemma. You will always go against one or more values. However, the fact that there is no 'right' answer does not mean that you cannot have a discussion or that some solutions would be better than others.

Security:

- A transferable share or other negotiable security or equivalent right, other than a right of ownership in immovable property in the form of an apartment right;
- A negotiable bond or other negotiable debt instrument;
- Any other transferable security issued by a legal entity, company or institution which gives the right to acquire a financial instrument as referred to in item (a) or (b), either by exercising the rights attached thereto or through conversion, or which is settled in cash;

Financial instrument:

A financial instrument as referred to in Section 1(1) of the Financial Supervision Act. Examples include securities, money-market instruments, rights of participation in a collective investment scheme or UCITS and similar. Within the framework of the Regulation on private investment, crypto-assets are also considered to be a financial instrument.

Data Protection Officer:

The Data Protection Officer is responsible for independently supervising the implementation of and compliance with the GDPR, as well as monitoring the in-house privacy policy.

Related third party:

A related third party refers to your spouse or partner, children, foster children, blood relatives and relatives by marriage in the direct line, first degree and second degree, and anyone else with whom you share a close personal connection.

Closed list:

The list of companies and/or financial instruments in respect of which the AFM currently possesses inside information.

Breach of Union law:

It is also possible for employees to report breaches of the law of the European Union, Union law. A breach of Union law is an act or omission that is unlawful or undermines its objective. This concerns acts of the European Union, i.e. EU regulations or directives, or national legislation derived from them, within certain policy areas. A full list of relevant policy areas is provided in Annex 2 of the Directive. See Annex 2 of Directive (EU) 2019/1937 of the European Parliament and the Council of 23 October 2019 on the protection of persons who report breaches of Union law. Examples include environmental protection or the protection of personal data.

Information about a breach:

Information, including reasonable suspicions, about actual or potential breaches of Union law, which have taken place or are very likely to

take place within the organisation where the reporting individual works or has worked or within another organisation with which the reporting individual has had contact by virtue of their work, as well as about attempts to conceal such breaches.

Insider:

An employee who has been designated an insider following registration as such by a project manager and/or compliance officer.

Integrity violation:

A breach of internal and/or external laws, regulations or core values, which could compromise the integrity of the employee. Integrity violations can take many forms, including: inappropriate conduct in matters related to the AFM, leaks of confidential information, theft, embezzlement, corruption, manipulation or misuse of information or access to information, wastage and misuse of AFM assets, use of (physical) violence, threats, intimidation and any other misconduct, whether punishable by law or not, conflicts of interests, incompatible positions, contacts or activities, or fraud. This enumeration is not exhaustive but it does provide an indication of what might constitute a breach of integrity in the context of the Code of Conduct.

Complaints Committee:

An internal committee, which is made up of a compliance officer and the general counsel.

Complainant:

The individual who has approached the confidential counsellor or submitted a complaint to the Complaints Committee regarding undesirable behaviour.

Vulnerable positions:

These are positions that entail additional risk of integrity breaches. Consider, for example, employees handling sensitive information or being in a position in which the employee is particularly exposed. In the latter case, such positions include management positions, i.e. first-tier and second-tier positions, the role of general counsel, senior supervisors, compliance officers and fine officers.

Employee:

- Anyone who has an employment agreement with the AFM;
- Anyone who carries out work for the AFM on a regular basis or is seconded to the AFM, such as external advisers, placement students and agency workers and temporary workers;
- Anyone who does not come under any of the above categories but who, for the purpose of the Code of Conduct and the Integrity Policy, has been designated an employee by the compliance officer.
- The members of the AFM Supervisory Board are also designated as employees within the framework of the Code of Conduct and the Integrity policy.

Reporting individual:

A natural person who, given their future, current or past work at the AFM reports an apparent or suspected integrity violation, undesirable behaviour or wrongdoing within the context of work-related activities.

Hotline:

The independent hotline which acts as hotline within the framework of the Regulation on reporting apparent or suspected wrongdoing, violations of integrity and undesirable behaviour. The hotline consists of the compliance officers.

Societal wrongdoing:

Societal wrongdoing occurs when an act or omission affects the public interest. Such an act or omission must display one or more of the following characteristics:

- it involves a violation of the law or of internal rules established by the AFM pursuant to a statutory provision;
- there is a threat to public health;
- there is a threat to the safety of individuals;
- there is a risk of environmental degradation;
- there is a threat to the proper functioning of the organisation as a result of an improper act or omission.

The public interest is, in any case, deemed to be at stake if the act or omission affects not just personal interests, but rather affects several individuals and involves either a pattern or structural issue, or if the act or omission is serious or extensive in nature.

Wrongdoing:

Wrongdoings fall into two categories:

- a breach of Union law: a breach of a regulation or directive of the European Union in specific policy areas.
- a societal wrongdoing.

Company subject to supervision:

Institutes, individuals or legal entities who are monitored by the AFM for compliance with the rules laid down by or pursuant to the Financial Supervision Act (Wft), the Money Laundering and Terrorist Financing (Prevention) Act (Wwft), the Financial Reporting (Supervision) Act (Wtfrv), the Audit Firms (Supervision) Act (Wta) and the Consumer Protection (Enforcement) Act, also including the European regulations supervised by the AFM by virtue of the EU Financial Markets Regulations (Implementation) Decree.

Undesirable behaviour:

Behaviour that is perceived as crossing a line and/or offensive and that is intended to make an employee no longer feel safe at their place of work, or has the effect of doing so. Examples:

- Discrimination (direct or indirect distinction): that someone is treated differently from another in a similar situation, or would be treated differently, on the grounds of religion, personal beliefs, political opinions, race, gender, nationality, heterosexual or homosexual orientation, civil status, age, handicap or chronic illness, or that an apparently neutral provision, measure, standard or procedure has a particular impact on anyone of a certain religion, personal beliefs, political opinions, race, gender, nationality, civil status, age, heterosexual or homosexual orientation, or with a handicap or chronic illness.
- Aggression and violence/intimidation: cases in which an employee is mentally or physically harassed, threatened or attacked in circumstances that are directly related to the performance of the work. Consider verbal violence (scolding, insulting), physical violence (e.g. kicking, hitting, threatening with a weapon and/or being mugged). It can also involve psychological violence: threats, intimidation, putting under pressure, threats in relation to a person's domestic situation, damaging property.
- Bullying: all forms of intimidating behaviour of a structural nature,

by one or more employees (colleagues, managers), aimed at an employee or group of employees who are unable to defend themselves against such behaviour: mocking through words or gestures, making work unpleasant or even impossible.

- Intimidation, including sexual harassment: any form of verbal, non-verbal or physical behaviour with a sexual or other connotation whose purpose or effect is to violate a person's dignity, in particular whenever an intimidating, hostile, degrading, humiliating or offensive environment is created.

Private investment transaction:

A transaction in a financial instrument for one's own account or for the account of a third party, either in part or in full, and which is performed other than in the execution of a role or position. The acquisition of a financial instrument by any other means, such as by way of a gift, is also deemed to constitute a private investment transaction.

Breach of Union law:

An act or negligence which is either unlawful and relates to Union action and directive-based policies, or which undermines the purpose or application of the rules in Union acts and policies. Examples include: public health, data protection, security of network systems and information systems, prevention of money laundering and terrorism financing, breaches related to the internal market. This refers to specific directives or regulations covering specific areas of Union law.

Conflicting interest:

A scenario in which the personal interests of an employee could influence or appear to influence the impartial and objective execution of their duties.

Tipping off:

The disclosure of inside information to any other person, except where such a disclosure is made in the normal exercise of one's duties, profession or role.

Transaction:

An agreement for the exchange of items or rights which involves the AFM.

Supervisory antecedents:

Such as incorrect or incomplete informing a supervisory authority, a licence denied or a formal or informal measure imposed on a company subject to supervision where the employee's role included involvement in or responsibility for policy setting or was employed in a second-tier position.

Suspicion of wrongdoing:

The reporting individual's suspicion that there is a wrongdoing in the organisation where they work or have worked, or in another organisation with which they came into contact through their work, provided that the suspicion is based on reasonable grounds derived from information that the reporting individual has acquired through the AFM or arising from the knowledge that the reporting individual has acquired through their work at another company or another organisation.

Confidential counsellor:

A confidential counsellor primarily acts as a sounding board and stands beside the employee. In addition to lending a listening ear, confidential counsellors can also contribute and give employees information about the different options in dealing with undesirable behaviour and integrity dilemmas.

Meetings with confidential counsellors are at all times confidential, unless there are criminal matters involved.

Benefits:

Gifts, discounts, vouchers, invitations, hospitality, such as lunches, dinners, travel expenses and hotel accommodation, and other favours.

Inside information:

Information that is specific, has not been made public, and directly or indirectly relates to one or more issuers or one or more financial instruments (such as shares or bonds) and which, if disclosed, could have a significant impact on the price of those financial instruments and/or the price of related derivative financial instruments.

Discretionary management agreement:

The execution or arranging of the execution of private investment transactions in financial instruments based on a written management agreement to that effect, concluded with a portfolio manager who has full discretionary power.

Work-related context:

Current or past work-related activities in the public or private sector through which, regardless of the nature of that work, persons may obtain information about breaches of Union law or wrongdoing and where those persons may face harm if they were to report such information.

Work instructions for updating the closed list:

These work instructions describe when an institute or a financial instrument is added to the closed list.