

Altera Management B.V.

C1. Code of Conduct

25 March 2026

A translation of this Code of Conduct is also available. The Code of Conduct was published in April 2026 established by the management of Altera.

Version control

Date of adoption	March 2026
Version	2.4
Date of reassessment	March 2028
Author	Frank Stockmann
Log File/Changes	August 2023: Implementation of suggestions for improvement from Board members. October 2023: Implementation of additional suggestions for improvement from Board members + translation of the EN Code of Conduct. November 2024: Implementation of feedback points received from the organization, including removal of the Supervisory Board from the definition of Data Subjects, in connection with the Supervisory Board's existing commitment to the Supervisory Board Regulations policy. April 2025: Review of implementation changes related to the FGR structure. Also, insider has been replaced by the person involved everywhere in the document. March 2026: Language errors have been removed. In addition, the threshold amount for reporting private renovation and real estate transactions has been changed from EUR 2,500 to EUR 5,000. Compliance Officer has also been replaced by Compliance. Finally, each chapter now ends with do's and don'ts.

Table of Contents

1. PURPOSE AND PRINCIPLES	3
2. DEFINITIONS	5
3. CLEAN DESK	6
4. USE OF EMAIL, SOCIAL MEDIA, AND THE INTERNET	8
5. MIXING OF PRIVATE AND BUSINESS INTERESTS AND PERSONAL INVESTMENTS	
5.1 Accepting business gifts, invitations, ancillary positions and participating in other companies and institutions	16
5.2 Provisions for data subjects	18
5.3 Notification and approval	19
5.4 Data retention and confidentiality	20
5.5 Unforeseen circumstances	20

1. PURPOSE AND PRINCIPLES

IMPORTANT INFORMATION

Altera Management B.V. (hereinafter referred to as "Altera"), in its capacity as independent authorised director, represents the custodians Altera Residential Custodian B.V. and Altera Retail Custodian B.V. (and the funds Altera Residential Fund and Altera Retail Fund) in the real estate sector through real estate ownership and management.

General

1. Altera disapproves of any form of discrimination, threats, humiliation or intimidation in the dealings between Data Subjects. This can involve bullying, (sexual) intimidation, exclusion, aggression, violence, etc. (undesirable behaviour). These behaviours are unacceptable and can have serious consequences for the well-being of the victim, the working environment and the reputation of Altera. Acting in violation of this (if proven) has disciplinary and employment law consequences for the person who is guilty of this (see Article 2). For more information about the desirable and undesirable behaviours within Altera, see our "Policy on (un)desirable behaviour". Altera also has a Complaints Procedure for reporting complaints about undesirable behaviour.
2. In the event of action contrary to Altera's business interests or the rules in the Code of Conduct, measures may be taken depending on the nature and seriousness of the violation. For you as a Data Subject, this includes disciplinary measures and employment law measures, such as a reprimand, transfer, suspension or termination of the employment contract. For Guests, such measures may include temporarily or permanently denying access to the network or the internet. Depending on the seriousness of the violation, a disciplinary and/or employment law measure will follow. The nature of the sanction to be imposed is determined by the management. In the case of a member of the Executive Board, the sanction is determined by the chairman of the Supervisory Board and the other members of the Supervisory Board. If it concerns the chairman or a member of the Supervisory Board, this is reported to the other Supervisory Board members.
3. As a result of Altera's activities, you as a Data Subject are likely to have access to inside information or other sensitive information, such as non-public information about investors, investments or about Altera's activities. As a Data Subject, you must handle this sensitive information with care and you must keep all this information strictly confidential.
4. The purpose of this policy is to help protect Altera against:
 - i. undesirable behaviour;
 - ii. disruption of proper business operations;
 - iii. damage to Altera's reputation;
 - iv. financial damage resulting from misuse or improper use of information; and
 - v. loss, theft and unwanted disclosure or damage to information and data carriers.
5. Both direct and indirect violation of the rules of the code of conduct is not allowed. As a Data Subject, you are therefore not permitted to involve Third Parties and Guests in actions that are in violation of the Code of Conduct.

6. Without prejudice to the general purport of the foregoing, as a Data Subject you may not use Altera on the basis of such sensitive information:
 - i. advising or inducing another person to enter into a transaction, other than in the context of the proper performance of his employment or service agreement;
 - ii. disclose information or opinions to another person other than in the normal course of his employment or service agreement.
7. In addition, as a Data Subject of Altera, you may not disclose to Third Parties any information of which you, as a Data Subject, have become aware in the course of the performance of its activities within Altera and the confidential nature of which is or should have been known to you as a Data Subject, with regard to, inter alia, but not limited to, the activities of Altera. investors in Altera and (potential) investments of Altera.

Specific procedures relating to public-private transactions and public investment

8. Documents relating to public-private transactions and public investments may only be shared within a limited group of Data Subjects.

Specific procedures regarding information received from companies

9. Data subjects should assume that all due diligence and other information received from companies and other counterparties contains material confidential information. In many cases, Altera is bound by strict confidentiality obligations and disclosing confidential information would likely be a breach of contract, which could lead to a claim for damages against Altera. Disclosing confidential information is not only a potential criminal offence (e.g. a violation of insider trading laws), but also a serious breach of trust and can have a negative impact on our relationships and reputation.

Recap

☒ DO'S

- Treat colleagues and relations with respect
- Report undesirable behaviour immediately
- Contribute to a safe working environment
- Keep confidential information strictly confidential
- Share information only with authorized people
- If in doubt, ask for advice from Compliance

☒ DON'TS

- Discriminate, intimidate or bully
- Engaging in aggressive or threatening behavior
- Ignoring unwanted behavior
- Sharing information with third parties
- Using Information for Private Purposes
- Trading on the basis of inside information

2. DEFINITIONS

In this policy, the following terms have the following meanings:

Board member	member of the board of directors at Altera
Data Subject Compliance	means Altera's Compliance function
Personal transaction	transactions as referred to in paragraph 5.2
Regulation	a legal act that is directly binding
Person(s) involved	management, all other employees employed by Altera and all other employees of Altera, persons designated as such by the management
Guests	visitors, clients, invited persons and other external parties who are temporarily be present at a location, event or within the Altera organisation
Third parties	spouses, partners, family and relatives and members of the household

Unless otherwise stated, any reference in this policy may be to:

- (a) refer to any Policy or any other document or instrument and include (without prejudice to any prohibition on modifications) any modifications and restatements thereof;
- (b) an amendment, an addition, renewal, rewording, or reintroduction and the word modify and its derivatives shall be construed accordingly;
- (c) inclusive shall not be construed restrictively, but means inclusive without limiting or detracting from the generality of the foregoing and the word inclusive and its derivatives shall be construed accordingly;
- (d) a person must be understood as including his successors in title, permitted successors and authorised transferees;
- (e) person, a person, firm, company, corporation, government, state or agency of any state or an association, trust, partnership or other entity (whether or not having separate legal personality) or two or more of the foregoing;
- (f) a legal provision (including EU Directives) or Regulation (including EU Regulations) is a reference to that provision as amended or re-enacted.

Section titles and paragraphs are for easy reference only.

In this policy, words and phrases that include the singular, where the context allows or requires it, the plural and vice versa, and words and phrases that import the masculine, where the context allows or requires it, include the feminine and neuter and vice versa.

3. CLEAN DESK

Rules regarding tidy desk

10. This section contains a number of standards that you, as a Data Subject, must observe when dealing with information and data carriers. Those involved must observe the rules regarding a tidy desk. Compliance with this helps to prevent damage to the integrity and reputation of Altera and you as a Data Subject.

Workplace

11. As a Data Subject, you are responsible for the way in which you deal with information and data carriers. As a Data Subject, you must always handle the information and data carriers entrusted in such a way that only authorized persons have access to this information and data carriers. After working hours, you as a Data Subject must take reasonable measures to store confidential information and data carriers in a safe place. In addition, as a Data Subject, you must store personal belongings in a safe place both during working hours and after working hours. Altera is not responsible for the loss or theft of personal belongings of the Data Subjects.

Meeting rooms

12. After meetings, all materials should be removed, discarded, or cleared from the meeting room or other meeting location. This includes overhead sheets, flipchart sheets, and writing on whiteboards. Those involved in the meeting are responsible for ensuring that all material is removed, discarded, or deleted.

Computer

13. When leaving the office, you as a Data Subject must close your mobile devices and laptop or log out. If applications are active that cannot be closed if this would interfere with the process of the application, you as the Data Subject must lock the operating system of your mobile devices and laptop. As a Data Subject, you must also lock your mobile devices and laptop when you leave your seat.
14. As a Data Subject, you may not in any way prevent the operating system from automatically locking the computer or updating the software after a certain period of inactivity.

Use of passwords

15. The use of usernames or passwords of other Data Subjects is not permitted. As a Data Subject, it is forbidden to share your username or password with others.

Software

16. The removal or installation of hardware, software or other equipment on the network by individual Data Subjects is not permitted without the permission of the Digital Manager or the designated representative of the IT department. As a Data Subject, you may also not download or otherwise install software. All software must be pre-authorized by the IT department or the designated IT department representative. Altera has installed virus scanning software on every computer. As a Data Subject, you may not disable this virus scanner software or change its settings. Altera has installed an automatic screensaver on every computer. As a Data Subject, you may not turn off this screensaver or adjust its settings. As a Data Subject, you must ensure that confidential information is stored in a proper manner (with due observance of the laws and regulations relating to the processing of personal data). In case of any software and data protection doubts, you as a Data Subject should contact the IT department or the designated representative of the IT department.

Working from home/using a private computer

17. If confidential business information is taken or used by a Data Subject outside the office, you as a Data Subject must ensure that this information is treated carefully and confidentially. As a Data Subject, you are not permitted to store confidential business information on a private computer.

Portable computers/laptops/smartphones

18. The IT department or the designated IT department representative must ensure that recent antivirus software is installed on portable computers/laptops/smartphones. Users of portable computers/laptops/smartphones should always ensure that the information they use is protected. Therefore, password-protected screensavers and, in the case of highly sensitive documents, password-protected document security should be used. The portable computer/laptop/smartphones must always be carried as carry-on baggage. A portable computer/laptop/smartphone should never be left unattended (e.g. a computer/laptop/smartphone in a car).

Recap

☑ DO'S

- Lock your laptop when you're away
- Store documents securely
- Use only approved software

✗ DON'TS

- Password sharing
- Leaving confidential information lying around
- Installing software without permission

4. USE OF EMAIL, SOCIAL MEDIA, AND THE INTERNET

19. Having regard to:

Articles 7:611 and 7:660 of the Dutch Civil Code, and the General Data Protection Regulation,

While:

- (a) Altera and its Data Subjects are obliged to deal with each other in the spirit of a good employer-Data Subject relationship (Article 7:611 of the Dutch Civil Code).
- (b) (Many of) Altera's Data Subjects need the internet and e-mail to carry out their work properly.
- (c) Social media, such as LinkedIn, offer Data Subjects the opportunity to show commitment to their work and to make a positive contribution to Altera's image.
- (d) Given the potential risks, rules are needed for the use of email, the internet and social media.
- (e) Against the background of these risks, Data Subjects are expected to use the internet, e-mail and social media in a responsible manner.
- (f) Altera is authorised to give instructions on the use of the internet, e-mail and social media and to take measures to ensure the smooth running of the business in the company (Article 7:660 of the Dutch Civil Code).
- (g) Altera is authorised to supervise, where necessary, the use of social media and the use of the e-mail and internet system made available by Altera in order to ensure compliance with this Code of Conduct.
- (h) In carrying out such monitoring, Altera shall take into account the fundamental rights and freedoms of the Data Subject(s) concerned, in particular the right to privacy.

Objective

20. The purpose of these rules in this chapter is to promote the responsible use of social media (both private and work-related) and of Altera's internet and e-mail system and to ensure that the monitoring of this use is in accordance with the protection of the privacy of Data Subjects.
21. The purpose of monitoring personal data in relation to the use of social media and the e-mail and internet system made available by Altera is as follows:
- coaching/individual assessment of Data Subjects;
 - gathering evidence and preserving relevant facts;
 - safeguarding Altera's good reputation and preventing negative publicity;
 - Combating improper use, for example for harassment, including sexual harassment, and discrimination;
 - ensure that trade secrets are protected/guarded;
 - guaranteeing the proper functioning of Altera's computer equipment and software;
 - supervising cost and capacity management.
22. Email messages can be monitored for one of the following purposes:
- to ensure business continuity in the event of absence, illness or dismissal of the Data Subject;
 - to solve IT problems (with the consent of the Data Subject);
 - to ensure business continuity in the event of an emergency.

General principles

23. Altera supports an open dialogue, the exchange of ideas and the sharing of knowledge through the use of social media and Altera's e-mail and internet system. Altera reminds its Data Subjects of their own responsibility.
24. Altera reserves the right, where necessary, to monitor its Data Subjects with regard to the use of social media and Altera's e-mail and internet system.
25. These rules regarding the use of e-mail, social media and the internet have been drawn up in accordance with the General Data Protection Regulation (GDPR – publishing personal data of another person on the internet).
26. Personal data will only be used for the purpose for which it was collected (see purpose above).
27. Data relating to the use of social media and the e-mail and internet system made available by Altera that can be traced back to an individual will not be recorded, collected, checked, combined or processed in any manner other than as agreed in this Code of Conduct. Situations not provided for in this Code of Conduct will be dealt with in accordance with the employment law framework and the General Data Protection Regulation.
28. Personal data about the use of social media and the e-mail and internet system made available by Altera are not stored longer than necessary, with a minimum retention period of 1 month, unless there is a legitimate interest that makes it necessary to extend this period.
29. The employer ensures that the IT service provider (DHS) performs its work for Altera with integrity.
30. The IT service provider is permitted, subject to permission from the management, to make users' personal data temporarily inaccessible if essential activities make this unavoidable. Unlike in acute emergencies, you as a Data Subject will be informed of this temporary inaccessibility.

Risks

31. Failure to strictly comply with the rules regarding e-mail, social media and the internet can lead to the following risks:
 - unauthorized persons gaining access to confidential data;
 - unauthorized persons who copy, modify, destroy and/or add data;
 - unauthorized use or installation of software;
 - overloading the network or memory of a computer;
 - increased sensitivity of the communication platform to viruses and malware;
 - disseminating information that is discriminatory, sexually harassing or threatening in nature.

32. The possible consequences of these risks are as follows:
- loss of information;
 - unintentional disclosure of confidential or sensitive information;
 - stagnation or cessation of business processes;
 - violation of software license agreements;
 - infringement of copyright;
 - significant financial loss;
 - negative publicity for the employer;
 - pressure on the working relationship between Data Subjects.

Email usage

33. As a Data Subject, you must use Altera's e-mail system for business purposes.
34. As a Data Subject, you have the right to use the email system for non-work purposes for a short time (sending and receiving both internal and external personal email messages), provided that such use does not disrupt or impair the progress and quality of the Data Subject's daily tasks, is not disruptive to others and does not adversely affect the operation of the network.
35. Professional and respectful communication applies to work-related email use.
36. As a Data Subject, you may not use the email system to send messages containing pornographic, racist, discriminatory, insulting or otherwise offensive content.
37. As a Data Subject, you may not use the email system to send messages containing content that is harassing/sexually harassing.
38. As a Data Subject, you may not use the email system to send messages that may incite hatred and/or violence.
39. It is forbidden to distribute chain letters, spam and viruses or to burden the e-mail system in any other way that would lead to an unnecessary load on the network and/or to disrupt the smooth running of the company.
40. In the interest of preventing spam, the Data Subject is not permitted to leave Altera e-mail addresses on the Internet, unless this is for work-related purposes.

Internet use

41. As a Data Subject, you must use Altera's internet system for business purposes. Consequently, its use is related to the performance of the tasks of the Data Subject.
42. As a Data Subject, you have the right to use the internet system for non-work related purposes for a short period of time, provided that such use does not disrupt or hinder the progress and quality of the Data Subject's daily tasks, is not disruptive to others and does not adversely affect the operation of the network.

- 43. Professional and respectful use applies to work-related internet use.
- 44. As a Data Subject, you may not use the internet system to download and store files for your own private use.
- 45. As a Data Subject, you may not use the internet system to intentionally visit websites that contain pornographic, racist, discriminatory, abusive or other objectionable material or that have a criminal background or intent (e.g. related to hacking). It is forbidden to download such material.
- 46. As a Data Subject, you may not intentionally visit gambling websites.
- 47. As a Data Subject, you may not engage in internet use that is unlawful or punishable. All legal prohibitions apply at Altera. For example, it is forbidden to use the internet system to illegally download or distribute images, programs and music files. Altera also preventively blocks the use of internet systems such as Wetransfer.
- 48. As a Data Subject, you may not seek unauthorized access to non-public sources via the internet system.

Work-related social media

- 49. Only if you have been designated by the Board of Management or the Head of Investor Relations as an authorised Data Subject (hereinafter referred to as "Authorised Data Subject(s)") may you be active on behalf of Altera on employment-related social media, such as Altera's LinkedIn page, in the context of your position.
- 50. Only as an authorized Data Subject may you share knowledge and standard company information via the work-related social media channels in accordance with the instructions provided.
- 51. As an authorized Data Subject, you must remain within your own area of work. In case of doubt, you as the Data Subject should contact the management.
- 52. As a Data Subject, you may not publish confidential information and/or business-sensitive information of Altera on work-related social media (unless permission has been obtained from the management or the Head of Investor Relations) or make any negative comments about Altera and/or its Data Subjects in any way.
- 53. As a Data Subject, you may not publish confidential and/or harmful information relating to Altera's business relationships (e.g. participants and/or customers and/or tenants and/or property managers and/or other parties with whom Altera has a business relationship) on work-related social media, unless prior permission has been obtained.
- 54. If, as an authorised Data Subject, you post messages on work-related social media that may be related to Altera, you must in principle state the organisation and your job title.

Private use of social media

55. As a Stakeholder of Altera, you may be active on your private social media for private purposes, provided that this use does not detract from your productivity for Altera or damage Altera's image.
56. As a Data Subject, you may not publish any work-related topics on your personal social media (this does not include the publication of general information about Altera and your position/position as a Data Subject at the company or the publication of work-related topics on personal social media that have already been posted on Altera's social media by the authorised Data Subject, such as sharing a message posted on Altera's LinkedIn page or website).
57. In the interest of preventing damage to Altera's image, as a Data Subject you may not make negative statements on your personal social media about Altera as an employer and/or its Data Subjects and about Altera's direct relationships.
58. As a Data Subject, you must be aware that you bear a responsibility in your private use of social media and that private opinions can easily be confused with Altera's official position. You have to be fully aware that anyone can read what you write.

Social media (general)

59. As a Data Subject, you are responsible for the content you publish on social media.
60. As a Data Subject, you must be aware of your relationship with Altera. You need to make sure that your use of social media is in line with general standards of decency.
61. As a Data Subject, you should be aware that published content will remain in the public domain indefinitely, even after that content has been removed. This may have consequences for Altera's image.
62. As a Data Subject, you must take into account image rights, copyright and the right to quote.
63. If there is the slightest doubt as to whether a publication is in breach of this Code of Conduct or contains information that may reflect negatively on Altera, you as the Data Subject should contact the management or the responsible department/Data Subject.
64. As a Data Subject, you should be the first to correct your own mistakes, without first editing or deleting previous messages. In doing so, the Data Subject must indicate that he is the person who edited the message.

Monitoring

65. Any monitoring of the use of social media and the e-mail and internet system made available by Altera constitutes the processing of personal data within the meaning of the General Data Protection Regulation.
66. Monitoring of the use of social media and the e-mail and internet system made available by Altera will only take place if this is deemed necessary in the context of the objectives referred to in Chapter 3.

- 67. In principle, the monitoring takes place at the level of aggregated traffic data that cannot be traced back to identifiable persons.
- 68. If you, as a Data Subject or as a group of Data Subjects, are suspected of violating the rules of this Code of Conduct, intensive, targeted (substantive) monitoring may take place for a certain (short) period of time.
- 69. Prior to the targeted (substantive) monitoring, Altera shall inform the Data Subject(s) concerned about the objectives and nature of the data to be monitored, the circumstances under which the data will be received and their rights as described in Article 19(h) of this Code of Conduct.
- 70. Occasionally, the employer may secretly monitor a Data Subject without informing the Data Subject in advance, but only if there is a compelling reason for doing so.
- 71. Data of persons who can invoke the right of non-disclosure on the basis of the confidential nature of their position are not checked.

Rights of the Data Subject

- 72. Right of access: As a Data Subject, you have the right to access recorded data relating to you. Requests for access will be granted within 20 working days.
- 73. Right to obtain copies: As a Data Subject, you have the right to obtain copies of all registered data relating to you within 20 working days.
- 74. Right to rectification: As a Data Subject, you have the right to correct or supplement factually incorrect information in the recorded data personally or through a third party. Decisions on requests for correction or completion are made within 20 working days. If a request for correction or addition is granted, the correction will take place immediately.
- 75. Right to be forgotten: As a Data Subject, you have the right to delete and destroy recorded data relating to you that is not or no longer relevant, factually incorrect or in violation of this Code of Conduct or a statutory provision. Decisions on requests for deletion and destruction of registered data are made within 20 working days. If such a request is granted, the respective recorded data will be deleted and destroyed immediately.

Recap

☒ DO'S

- Use of systems primarily for business
- Communicate professionally and respectfully
- Think before you publish
- Distinguish between private and work
- Use social media responsibly
- Consult when in doubt
- Respect the privacy of others

☒ DON'TS

- Spreading abusive or illegal content
- Unauthorized downloading
- Sharing confidential information via social media
- Making negative or harmful statements
- Sharing confidential information
- Posting on behalf of Altera without permission
- Abusing systems
- Violating privacy rules

5. MIXING OF PRIVATE AND BUSINESS INTERESTS AND PERSONAL INVESTMENTS

Purpose

76. The purpose of the rules on the mixing of private and business interests and personal investments is to safeguard and maintain the confidence of stakeholders in Altera by encouraging desirable behaviour and preventing undesirable behaviour. These rules provide guidelines for the target group defined in Article 80 to prevent conflicts between Altera's interests and your private interests as a Data Subject, as well as to prevent the use of Altera's confidential information for private purposes.
77. The starting point is to promote transparency and ensure that all Data Subjects, including for their own protection, are clear about what is and is not allowed in terms of business interests and personal investments.
78. The rules on the mixing of private and business interests and personal investments are also intended to contribute to the integrity of Altera's functioning for the benefit of all stakeholders and to safeguard Altera's good name and reputation. Altera's management is responsible for complying with the obligations arising from a statutory provision or a provision of the Code of Conduct.

Standards

79. As a Data Subject, you are expected to behave with integrity (act carefully, explainably and steadfastly) and to behave in accordance with the highest standards of business ethics under all circumstances. This means, among other things, that all parties involved must prevent their private interests from coming into conflict with each other or becoming intertwined with Altera's interests, or from creating the appearance that this may be the case. This applies to all contacts with Third Parties.

Target group

80. This part of the Code of Conduct also applies to you as a Data Subject of Altera.
81. Both direct and indirect violation of the rules of the code of conduct is not allowed. As a Data Subject, you are therefore not permitted to involve Third Parties in acts that are in violation of the Code of Conduct. For the purposes of this Code of Conduct, "Third Parties" always include spouses, partners, family and relatives and members of the household.

Compliance

82. For the activities arising from the Code of Conduct, the Whistleblower Policy, the Undesirable Behaviour Policy, the Internal Complaints Procedure, the Incident Procedure and the Reporting of Unusual Transactions to FIU the Netherlands, the compliance function is carried out by Compliance at Altera (F. Stockmann).

Confidentiality

83. As a Data Subject, you may not disclose or disclose to others any confidential information about matters relating to Altera in general, or about investments that have come to your knowledge in the course of your employment, other than for the benefit of and in the interest of the company.
84. Nor may confidential information be used or attempted to be used for the benefit or benefit of others. Confidential information is defined as information that is not publicly accessible. In addition, as a Data Subject, you are obliged to maintain strict confidentiality with regard to the personal data of Third Parties to which you have access as a Data Subject for your work.

5.1 Accepting business gifts, invitations, ancillary positions and participating in other companies and institutions

Where prior approval under this Chapter is not reasonably possible, the notification shall be made as soon as possible retrospectively.

Accepting business gifts, invitations, etc.

85. As a Data Subject, you must avoid ending up in a situation in which accepting a business gift or invitation to (any form of) entertainment offered by a business relation or (possible) future relationship can influence your decisions. It is not allowed to create the appearance of influence.
86. Therefore, as a Data Subject, you must be careful and attentive when accepting and reporting business gifts and invitations. Attempts by (future) relations to improper influence must also be reported immediately. See also Section 5.3 for notification and approval.

Ancillary positions

87. Subject to approval (see Section 5.3), it is not permitted to hold ancillary positions such as supervisory boards, advisory positions, membership of investment committees, etc. at companies and institutions with which Altera maintains business contacts. The acceptance of ancillary positions at other companies and institutions is also subject to approval (see paragraph 5.3). When considering whether approval is granted, the guiding principle will be whether there are any ancillary positions that have or may conflict with your position as a Data Subject within Altera.
88. Ancillary positions that are related to a participation or participation of the company in which you as a Data Subject have been formally appointed or nominated by virtue of your position and where it is absolutely clear on the basis of which you as a Data Subject perform this additional position on behalf of the company, do not fall under the aforementioned prohibition.

Financial interests in business relationships

89. As a Data Subject, you may not have any financial interests in a company or institution with which Altera does or is likely to do business.

Suppliers/contractors, etc.

90. Use for the private activities of suppliers, contractors, brokers, maintenance services and/or other business service providers with whom Altera maintains business contacts is not permitted, unless approved after notification (see section 5.3).
91. Approval is only granted if no alternatives are possible, private financial benefit is excluded and the work is carried out under market conditions.

Assets of Altera

92. Without the prior consent of your Executive Board, the use of goods (of the funds and of the management organisation) of Altera for your own benefit is not permitted. Examples include office supplies, laptops, software, and intellectual property. The intellectual property of specific investment vehicles or analysis models developed by the company that have not been made public should be treated accordingly. Use for one's own purposes or disclosure to Third Parties is not permitted without the prior consent of the Executive Director.

Value and notification of gifts

93. The receipt of gifts, for example on the occasion of the New Year, should be limited to small gifts that do not exceed the commercial value of approximately €75 (per relationship per year). These gifts do not need to be reported. Gifts above € 75 (per relation per year) must be reported. See Section 5.3 for notification and approval. The management may decide to have the promotional gift returned.

Giving business gifts

94. Business gifts to Third Parties are never given, except insofar as the trade value does not exceed € 75 (per business partner per year).

Invitations

95. Invitations to travel, seminars, company visits and other meetings in the Netherlands or abroad will only be accepted after approval (see section 5.3 for notification and approval). In order to guarantee the independence of Guests, the travel and accommodation costs incurred by you as a Data Subject are always borne by Altera, unless otherwise determined after notification and approval (see section 5.3).

Acceptance

96. An invitation can never be accepted if there is a potential conflict of interest. It is also not permitted to accept money, goods or services in any form from Third Parties, except as provided for in Articles 93 and 95. See Section 5.3 for notification and approval.
97. Examples of what is illegal:
- travel (airline tickets, train tickets, transit tickets for travel by ship, hotel, apartment or holiday accommodation, rental cars);
 - expense allowances for partners;
 - supplies of goods or services at unusually high discounts or at non-market rates;
 - loans from business associates, etc.

Prerequisites

98. As a Data Subject, you may not trade in financial instruments in a business or private manner while you have inside information. The following transactions are exempt from reporting and monitoring:
- transactions in bonds issued by the State and other public authorities;
 - transactions in financial instruments the management of which has been transferred to a professional asset manager on the basis of a written agreement, on such terms that the person concerned cannot influence the selection of the fund or the transactions;
 - transactions in index funds or in listed units in (semi) open-ended investment funds, provided that the person concerned does not hold a position within that institution.
99. Trading means buying and selling, as well as subscribing to issues of financial instruments. Financial instrument means:
- securities, stocks;
 - money market instrument;
 - crypto's;
 - units of a collective investment undertaking other than a securities or investment company;
 - derivative contract, including, but not limited to, an option;
 - forward, swap, currency and forward rate contracts;
 - other financial instruments within the meaning of the Financial Supervision Act;
 - in addition, everything that is considered as such in the opinion of society.

Reporting of (potential) conflicts of interest

100. As a Data Subject, you are obliged to report any (potential) conflict of interest to Compliance. If you, as a Data Subject, have doubts about the applicability of the Code of Conduct or its interpretation, you should consult Compliance. If the (potential) conflict of interest relates to one of the members of the Executive Board or a member of the Supervisory Board, Compliance must report this to the Chairman of the Supervisory Board of Altera. In the case of the chairman of the Supervisory Board, this is reported to the other Supervisory Board members.

Signature and annual declaration of conformity

101. Everyone who joins Altera or otherwise joins the circle of Data Subjects receives the Code of Conduct and must sign a declaration of compliance with the Code of Conduct. As a Data Subject, you must then sign a declaration of compliance with the Code of Conduct at the beginning of each year. The signed statement of compliance with the code is provided to Compliance on an annual basis.

5.2 Provisions for data subjects***Business relationships***

102. A data subject is a person associated with Altera who is directly or indirectly involved in Altera's transactions, or who otherwise has or may have inside information by virtue of his/her activities, profession or position. A data subject is also the connected person who may have access to other confidential (market) information.

103. The data subject is not permitted to carry out private transactions with or through the intermediary of natural persons with whom the data subject has a business relationship. Private transactions involve the trading of financial instruments.

Indirect transactions

104. The above provisions of Article 103 apply, with reference to the provisions of paragraph 5.3, regardless of whether the person is acting (directly or indirectly through participations, managers or other Third Parties with the exception of freehand transactions):
- for themselves or for others;
 - alone or in cooperation with others;
 - knowingly or unknowingly with inside information that can be assumed to have it.

Private real estate transactions

105. As a data subject, you are obliged to immediately report (intended) personal real estate to Compliance in writing (by e-mail is sufficient). Compliance establishes this. In the case of (intended) renovation projects of more than €5,000 but no more than €25,000 within an expected period of 12 months, you as a data subject are obliged to check whether the contractor or supplier is currently working for Altera or has worked for Altera in the past 12 months, in order to assess possible conflicts of interest. As a data subject, you then contact the person concerned from PFM Residential / Retail. Renovation projects also include the installation of solar panels, a dormer window, a kitchen or a bathroom. If the conclusion is that there is a contractor or supplier of Altera, you must report to Compliance why you believe there is no conflict of interest. If the (intended) renovation projects exceed €25,000 within an expected period of 12 months, you as a data subject are always obliged to report this immediately in writing (by e-mail is sufficient) to Compliance.

5.3 Notification and approval

106. Notification and obtaining approval is the responsibility of every person associated with Altera. Compliance acts as an advisor to the extent necessary, and as a manager in the light of the monitoring activities that arise from the supervision of compliance with the Code of Conduct. Compliance immediately receives a copy of the registration of reports for the purpose of checking compliance with the code of conduct (e-mail is sufficient). If a notification obligation arises on the basis of the above or approval must be requested, the following procedure applies:

Notification to Compliance (and Chief Financial Officer)

107. As a Data Subject, you report and/or request written approval to Compliance in the case of all of the aforementioned reports.
108. Compliance then reports all reports made and/or Compliance requests approval of all requests from the management and records this in writing.
109. As a Data Subject, you are obliged to immediately report any (potential) conflict of interest or reputational risk to your Executive Board member and Compliance. Attempts by a (future) relationship to influence must also be reported immediately to the management in accordance with the above.

Notification to your own manager and (line) director

110. As a Data Subject, you request permission in writing (by e-mail) from your own manager and/or his/her (line) Board member for a gift with a value of more than € 75 (as referred to in Article 93) or an invitation (as referred to in Article 95). After written permission (by e-mail is sufficient) from the above-mentioned persons, you as a Data Subject register them yourself on the "gifts/invitation list" that has been made available in a generally known accessible place (Compliance Teams in the gifts and events calendar channel).
111. If in doubt about notification or approval, ask Compliance for advice. The "gift/invitation list" is periodically discussed in the Risk & Compliance meeting.

5.4 Data retention and confidentiality

112. Your Data Subject notification and/or approval data will be retained for a maximum of five years. Compliance and the Management are obliged to maintain the confidentiality of the information provided by Data Subjects or Third Parties (with the exception of notifications about gifts and invitations that are placed on an internally accessible list).

5.5 Unforeseen circumstances

113. The Executive Board decides on matters that do not fall under this Code of Conduct.

Recap

☑ DO'S

- Report (potential) conflicts of interest immediately
- Be transparent about ancillary positions
- Reporting gifts > €75
- Be cautious with invitations
- Trade Transparently
- Follow compliance procedures
- Reporting relevant transactions as described in section 5.2

✗ DON'TS

- Letting private interests play a role
- Doing business with your own network without notification
- Allowing situations to exist that give the "appearance of a conflict of interest"
- Accepting gifts that can have an impact
- Ignoring the obligation to report
- Insider trading
- Investing in conflicting parties
- Circumventing the obligation to report

This policy is evaluated every two years (or more often if necessary).