
COMPLIANCE POLICY

Dated 15 July 2021

ALTERA VASTGOED N.V.

This Compliance Policy including its Annexes (the **Policy**) is adopted by the board of directors (*het bestuur*, hereinafter: the **Board**) of Altera Vastgoed N.V. (**Altera**) on 15 July 2021.

PART 1: INTRODUCTION

Subject

- 1 Capitalized terms used but not defined in (the body of) this Policy shall have the meaning as set out in **Annex I**. This Policy shall be construed as set out in **Annex I**.
- 2 This Policy describes (i) the composition, functioning, tasks and responsibilities of the compliance function of Altera, and (ii) certain responsibilities and obligations of employees of Altera in the area of compliance.
- 3 This Policy is established for the purpose that Compliance is important for Altera. The vision and mission of Altera is that we work from our core values: “clear, thoughtful, optimistic, committed, honest, decisive”. The interest of the shareholders always come first for us. Conflicts and conflict of interest are avoided. Investing in a responsible manner is important to us: real estate investments must be good for the investor, the tenant and society.
- 4 That is why maintaining and promoting the integrity of the organization, its employees, its customers, its data and the market is important to Altera. This Policy is complying with sections 4:9, 4:11, 4:14, 4:15a and 5:68 AFS and implementing articles 7, 12 and 18 AIFMD and the rules of the Regulation promulgated thereunder (in particular articles 61 and 63 of the Regulation).

Structure and contents

- 5 This Policy consists of the following PARTS and Annexes:

PART 1:	Introduction
PART 2:	Permanent Compliance Function
PART 3:	Development and implementation
PART 4:	Review; amendments
PART 5:	Support and Advice; Enforcement
PART 6:	(no) Internal Audit Function
PART 7:	Notifications to Competent Authorities
PART 8:	Code of Conduct
PART 9:	Oath or Solemn Affirmation
Annex I:	Definitions; Construction
Annex II:	Template Oath or Solemn Affirmation
Annex III:	Confidential Information

Annex IV: Clean Desk

Annex V: Use of Email and Internet

Annex VI: Mixing Private and Business Interests and Personal Investment Transactions

Annex VII: Cluster Munition

Annex VIII: Compliance policies and procedures acknowledgement form

Annex IX: Incident Notification Form

6 The requirements of the AIFMD are addressed in this Policy and the following policies (collectively, together with this Policy, the **Policies**):

- (a) this Compliance Policy;
- (b) the Conflict of Interest Policy;
- (c) the Remuneration Policy;
- (d) the Risk Management Policy;
- (e) the Transparency Policy;
- (f) the Service Provider Policy;
- (g) the Valuation Policy;
- (h) the AML/KYC Policy; and
- (i) the AO/IC Guide.

7 This Policy shall be applied separately and independently of, and without prejudice to the policies and procedures as set out in the (other) Policies.

Responsible Persons

8 The Compliance Officer shall ensure that this Policy is duly executed. The Compliance Officer shall be responsible for monitoring the compliance with this Policy.

Maintenance of the Policy and review

9 The Responsible Board Member shall ensure that this Policy, as well as any updates thereof, are made available to all (relevant) members of staff of Altera.

10 The Responsible Board Member together with the Compliance Officer shall review this Policy at least once a year on effectiveness, adequacy and whether or not it is still up-to-date, and shall report the findings of its review to the Board, in accordance with **Part 4**. The

Compliance Officer shall ensure that any such report is kept in a durable medium such that it remains available for inspection by Altera and the Competent Authorities.

PART 2: PERMANENT COMPLIANCE FUNCTION

Sufficient Resources and Expertise

- 11 The Board shall appoint one or more person(s) as the Compliance Officer. The board ensures that in all time a compliance officer is in place (whether the compliance officer will be hired externally or is employed by Altera). The compliance officer will be supported by the Responsible Board Member.
- 12 The Board shall ensure that the Compliance Officer (including any replacement):
 - (i) can act independently in the performance of the Compliance Function;
 - (ii) is competent and knowledgeable on the laws and regulations applicable to Altera or a specific area of law and regulation to be especially entrusted to him or her;
 - (iii) has sufficient seniority and authority;
 - (iv) is not involved in the performance of services or activities he or she monitors or mitigate conflicts if this should be the case; and
 - (v) has a remuneration which is not or not likely to affect his or her objectivity.
- 13 The Board shall ensure that, on an – as needed – basis, funds are made available to (or to the order of) the Compliance Officer to follow the courses and training on upcoming law and regulations reasonably required to fulfill the Compliance Function.
- 14 The Compliance Officer may engage at his discretion and after consultation with the Responsible Board Member, outside legal counsel to advice or assist on compliance topics, and its duties under this Policy.

Compliance Officer

- 15 The Compliance Officer shall take reasonable steps to promote compliance by Altera staff with this Policy and the (other) Policies and to respond to inappropriate or unusual actions by such persons (i.e. “red flags”) and to respond to questionable conduct brought to his attention.
- 16 The Responsible Board Member together with the Compliance Officer shall ensure that all Altera employees are informed on an annual basis, thereafter of the Policies and their notification obligations under the Policies.

- 17 The Compliance Officer is responsible for reporting on a frequent basis, and at least annually, to the Board on matters of compliance in accordance with paragraph 26.
- 18 The Compliance Officer acts as liaison with the Competent Authorities. The Compliance Officer may however authorize other persons to maintain contact with the Competent Authorities on well-defined topics (such as reporting).

Compliance Function

- 19 In order to detect any risk of failure by Altera to comply with applicable law and regulation, including the AIFMD, and the associated risks thereto, and to minimize such risk, the Compliance Officer shall perform the following functions (the **Compliance Function**):
- (i) the development and implementation of policies and procedures to ensure compliance by Altera of applicable law and regulations, including the AIFMD in accordance with **Part 3**;
 - (ii) the monitoring and review of the Policies on their effectiveness and completeness in accordance with **Part 4**;
 - (iii) the rendering of support and advice to the responsible persons designated in the (other) Policies, as well as members of staff of Altera, on their questions on compliance with applicable law and regulation, including the AIFMD and the Policies in accordance with **Part 5**; and
 - (iv) the monitoring and enforcement of compliance by members of Altera staff with the Policies in accordance with **Part 5**.

PART 3: DEVELOPMENT AND IMPLEMENTATION

Code of Conduct; Internal Audit Function; Notification(s) to Competent Authorities

- 20 In order to comply with applicable law and regulations, including the AIFMD, the Compliance Officer together with the Responsible Board Member have developed (or further developed, as the case may be) and implemented the Policies, as well as the code of conduct as set out in **Annexes III through IX** (collectively, the **Code of Conduct**), an assessment on the Permanent Audit Function as set out in **Part 6** and the policy on notification of the Competent Authorities as set out in **Part 7**.

Continuing Development and Implementation

- 21 If deemed necessary by the Compliance Officer or the Responsible Board Member, further policies and procedures continue to be developed by the Compliance Officer and Responsible Board Member in accordance with PART 4 upon:

- (i) a proposed change or restructuring of the business activities of Altera or its affiliates, including a launch of a new business activity, for instance the management of AIFs with strategies and or asset classes other than the ones of the existing private equity, a new AIF, individual asset management services or provision of ancillary services within the meaning of section 6 sub 4 AIFMD;
- (ii) a proposed change in Alteras staff and/or functions (unless such change is deemed irrelevant for the purpose of ensuring that persons engaged in business activities involving a risk of Conflict of Interest carry out their activities with an adequate degree of independence), delegation or outsourcing structures, or administrative organisation and internal control framework;
- (iii) a proposed change of applicable legislation or interpretation in relation thereto;
- (iv) a proposed change to any Policy other than this Policy;
- (v) the Compliance Officer receiving a notification of an incident or non-compliance of applicable law of regulation pursuant to paragraph 33;
- (vi) the Compliance Officer is (otherwise) made aware or himself becomes aware of a pending, threatened or potential incident or non-compliance with applicable law or regulation.

Notification on Change of Existing Manual or Policies

- 22 Any Altera employee who has been designated as a responsible person under a Policy other than this Policy shall notify any proposed change to such Policy promptly to the Compliance Officer and the Responsible Board Member timely prior to the proposed effective date of such change.

- 23 The Compliance Officer shall coordinate with the responsible persons under a Policy other than this Policy on the appropriate course of action. In case of conflicting opinions on the appropriate course of action to be undertaken, the Compliance Officer shall refer the matter to the Board, who shall decide on the matter.

PART 4: REVIEW; AMENDMENTS

Periodical Review; Incidental Review

24 The Compliance Officer shall review periodically, at least once a year, and further upon the occurrence of an event or circumstance set forth in paragraph 21 or at such occasion deemed appropriate or advisable by it, review whether the procedures and measures embedded in this Policy and the (other) Policies are:

- (i) adequate and effective, in light of applicable law and regulations;
- (ii) up-to-date; and
- (iii) complied with by the responsible persons set out therein and by Altera staff.

Access to Information

25 The review takes place on the basis of such information as deemed appropriate by the Compliance Officer, and may be collected by means of:

- (i) interviews with the Policies' responsible persons or any other Altera staff;
- (ii) review of documents and reports produced as described in the Policies; and/or
- (iii) on-site inspections.

Reporting

26 The Compliance Officer shall report the findings of its review to the Board. The Compliance Officer shall in an annual meeting discuss the outcome of the annual review with the Board.

Amendments

27 If it is concluded in the report that the procedures and measures embedded in this Policy or any other Policy are in-effective, insufficient, out-of-date or not complied with, the Compliance Officer propose amendments thereto to the Board. The Compliance Officer shall notify the responsible persons under a Policy other than this Policy of any proposed amendments timely prior to the proposed effective date of such amendment.

28 The Compliance Officer shall ensure that any amendments approved by the Board as referred to in the preceding paragraph are duly reflected in the relevant Policy or Policies and that any updated versions thereof are made available to all relevant members of staff of Altera in accordance with paragraph 29.

PART 5: SUPPORT AND ADVICE; ENFORCEMENT

Acknowledgement by employees

- 29 The Compliance Officer shall ensure that each MT member of Altera must complete a compliance policies and procedures acknowledgement form stating that he or she has received a copy of the Policies (or any update thereof) and that he or she has read and understands the Policies (or any update thereof), and that he or she shall comply with the Policies (and any update thereof).
- 30 A template of the acknowledgement form is attached as **Annex VIII**.

Training; Advice

- 31 The Compliance Officer together with the Responsible Board Member shall – on an as needed basis – ensure that responsible persons designated in the (other) Policies, as well as members of staff of Altera, are informed of the relevant developments in respect of the law and regulations applicable to Altera or its staff, either by giving or arranging for training sessions or by circulating emails, notes, newsletters or legal alerts of legal advisors and Competent Authorities, etc.
- 32 The Compliance Officer shall advise the responsible persons designated in the (other) Policies, as well as members of staff of Altera, on their questions on compliance with applicable law and regulation, including the AIFMD and the Policies.

Incident Notification

- 33 Any Altera employee who believes that an incident (whether or not material) involving applicable laws and regulations, and/or this Policy or any other Policy may have occurred shall report such incident promptly to the Compliance Officer through the incident notification form attached as **Annex IX**.
- 34 Incidents are irregularities which are or can be a serious danger for the integrity of Altera, and may be the result of the conduct of:
- (a) an employee or a member of the Board; or
 - (b) a person or an entity performing activities for or on behalf of Altera.
- 35 These irregularities may include: breaches of laws and legislation, breaches of Policies, fraud, corruption, and other undesirable behavior.

Internal reporting and recording

- 36 Incidents have the potential to affect the integrity of both individuals and Altera. Therefore an incident must be treated with due care. The Compliance Officer will be responsible for the supervision of compliance with this procedure and the handling of the incident.

- 37 Each employee is required to report an incident as soon as possible to the Compliance Officer. The Compliance Officer records the incident. The record on the incident should contain at least the following information:
- (a) the date of the incident;
 - (b) the characteristics of the incident;
 - (c) the identity of the persons that perpetrated, aided or abetted the incident; and
 - (d) the measures taken in response to the incident.
- 38 The Compliance Officer reviews the report and reports the incident to the Board as soon as possible. If necessary the Compliance Officer decides on starting an investigation in accordance with paragraph 42. If that is the case the Compliance Officer explains the nature of the investigation and working method to the Board. If the Compliance Officer believes that the Board does not cooperate sufficiently or the Compliance Officer has any indications that one of the Board members are involved in the incident, then the Compliance Officer will escalate to the Chairman of the Supervisory Board.
- 39 The Compliance Officer registers all incoming reports, the handling of the incident, the investigation, the results of the investigation, the preventive and corrective measures taken as well as the report to the AFM where required.

Confidentiality & non-retaliation

- 40 The Compliance Officer shall ensure the confidentiality of any employee within Altera who reports an incident in accordance with paragraph 37, in the event that such confidentiality is requested by the relevant employee.
- 41 Employees who report an incident in accordance with this Policy and in good faith will be given protection and shall not be put at a disadvantage because of the reporting.

Investigation

- 42 The aim of the investigation is:
- (a) to establish the facts on the incident and to collect evidence for legal procedures;
 - (b) to limit (potential) damage; and
 - (c) to take corrective measures regarding operations if necessary.
- 43 The Compliance Officer shall, if appropriate and in consultation with the Board and – if applicable – the relevant Policies' responsible persons, investigate any possible violations of applicable laws and regulations and/or this Policy or any other Policy that he becomes aware of. The report will contain at least a short summary of facts and

circumstances and an assessment of the incident as well as an advice on the measures he deems necessary.

- 44 Where an incident relates to a Policy which itself caters for an investigation procedure, the Compliance Officer may decide that such procedure is followed (instead of this procedure), provided that the Compliance Officer receives frequent updates of such procedure and that it shall at any time be authorized to take over such procedure. If the Compliance Officer commences an investigation, he will inform the Board. In addition, the Compliance Officer will discuss with the Board whether to retain outside counsel (or recommend to the Board that outside counsel be retained). The Compliance Officer shall have full authority to initiate an investigation, and the Board will have the authority to impose disciplinary or other sanctions, including a written warning, suspension, transfer or dismissal.

Measures

- 45 The Compliance Officer and a member of the Board (and where necessary supplemented with external legal counsel) will generally make up the incident team, which reviews the results of the investigation results and issues an advice to the Board with respect to:
- (a) Legal action or disciplinary measures against the employee(s) involved;
 - (b) Internal and external communication;
 - (c) Adjustment of procedures and measures in accordance with paragraph 21;
and
 - (d) Other corrective measures regarding the operations.
- 46 Measures and sanctions to be taken will be based on the premises that a serious violation will be harmful to the relationship between the employee and Altera. Causing an incident or being otherwise involved can therefore lead to disciplinary or other measures. In case of deliberate and/or serious criminal offences the authorities will be informed.
- 47 The incident team reports to the Board who will make a decision based on the facts and circumstances.
- 48 The Compliance Officer will be responsible for the handling of the incident.

PART 6: (NO) INTERNAL AUDIT FUNCTION

- 49 In light of the nature, scale and complexity of its business and the nature and range of collective portfolio management activities undertaken in the course of that business, Altera has not established an internal audit function.
- 50 The Compliance Officer together with the Responsible Board Member shall review once a year as part of its periodical review whether the assessment on the absence of the internal audit function is still valid.

PART 7: NOTIFICATIONS TO COMPETENT AUTHORITIES

- 51 Altera shall in accordance with applicable law and regulation, in particular Chapter 9 of the Decree, notify the Competent Authorities of any material change to the conditions of initial authorization, in particular material changes to the following information prior to the effectuation thereof:
- (i) information on the persons effectively conducting the business of Altera (i.e. the Board), including new appointments, and change in antecedents which may affect their trustworthiness, to the extent Altera is aware thereof in the normal course of its business, immediately after Altera has become aware thereof;
 - (ii) information on the identities of Alteras shareholders or members, whether direct or indirect, natural or legal persons, that have qualifying holdings and on the amounts of those holdings;
 - (iii) the program of activity setting out the organizational structure of Altera, including information on how Altera intends to comply with its obligations under Chapters II, III, IV, and, where applicable, Chapters V, VI, VII and VIII of the AIFMD;
 - (iv) information on the remuneration policies and practices pursuant to Article 13 AIFMD;
 - (v) information on arrangements made for the delegation and sub-delegation to third parties of functions as referred to in Article 20 AIFMD; and
 - (vi) such further notifications as listed on Annex VIII of the Transparency Policy.

PART 8: CODE OF CONDUCT

Requirement to comply

52 Employees of Altera are required to comply with the Code of Conduct.

PART 9: OATH OR SOLEMN AFFIRMATION

Obligation to take oath or solemn affirmation

- 53 Altera falls within the scope of the so-called “oath or solemn affirmation” obligation pursuant to the AFS and the Regulation Oath or Solemn Affirmation Financial Sector (*Regeling eed of belofte financiële sector 2015*), and is therefore obligated to ensure that Qualifying Individuals who work for Altera take an oath or make an affirmation in respect of the execution of their function within the financial sector ethically and with care.
- 54 Each Qualifying Individual is therefore obligated to take the oath or make the affirmation as set out in his or her Oath or Affirmation Form within three months of their commencement of the work for Altera. The Qualifying Individual may choose to either take the oath or make the affirmation (each, the **Oath**).
- 55 The Oath will be made before a member of the Board or, in the event that this is not possible, another natural person working for Altera before whom the Oath can be made in a meaningful way.

Procedure oath or solemn affirmation

- 56 For each Qualifying Individual an Oath or Affirmation Form will be filled out by including the name of the Qualifying Individual and the date and location of the oath or solemn affirmation.
- 57 The Oath will be made as follows:
- (i) the natural person before whom the Oath is made will read aloud verbatim the opening sentence and the text included under (a) – (h) of the Oath or Affirmation Form;
 - (ii) subsequently, the Qualifying Individual will say aloud verbatim either:
 - (a) “So Help me God!”; or
 - (b) “This I pledge and promise!”
 - (iii) lastly, the Oath or Affirmation Form is signed by the Qualifying Individual.
- 58 Altera will keep the signed oath or solemn affirmation form in a durable medium readily accessible for at least the duration that the Qualifying Individual works for Altera.

ANNEX I

DEFINITIONS; CONSTRUCTION

In this Policy, the following terms shall have the following meanings:

AFS	the Dutch Act on the financial supervision (<i>Wet op het financieel toezicht</i>), as well as the rules and regulations promulgated thereunder;
AFM	means the Dutch Authority for the Financial Markets (<i>Stichting Autoriteit Financiële Markten</i>);
AIF	means an alternative investment undertaking within the meaning of Article 4 AIFMD;
AIFMD	means Directive 2011/61/EC;
AML/KYC Policy	means the anti-money laundering / know-your-customer policy of Altera implemented by the Board, as amended from time to time;
AO/IC Guide	means the administrative organization guide of Altera;
Board	means the management board of Altera;
Code of Conduct	shall have the meaning as set forth in paragraph 20;
Competent Authorities	means the AFM and DCB;
Compliance Officer	means the compliance officer of Altera, being Rina Smaal;
Conflicts of Interest Policy	means the conflicts of interest policy of Altera, implemented by the Board, as amended from time to time;
Decree	Decree on conduct of business supervision financial undertakings Wft (<i>Besluit gedragstoezicht financiële ondernemingen Wft</i>);
DCB	means Dutch Central Bank (<i>De Nederlandsche Bank N.V.</i>);
Oath or Affirmation Form	means a filled out template oath or solemn affirmation form as included in Annex II ;
Personal Transaction	Transactions as mentioned in Annex VI ;
Qualifying Individual	means a person who is designated as Identified Staff in the Remuneration Policy of Altera;

Regulation	means the Commission Delegated Regulation (EU) No 231/2013 of 19 December 2012 promulgated pursuant to the AIFMD;
Remuneration Policy	means the remuneration policy of Altera, implemented by the Board, as amended from time to time;
Responsible Board Member	means the member of the Board responsible for compliance and risk management within Altera, being Cyril van den Hoogen;
Risk Management Policy	means the risk management policy of Altera, implemented by the Board, as amended from time to time;
Transparency Policy	means the transparency policy of Altera, implemented by the Board, as amended from time to time;
Service Provider Policy	means the service provider policy of Altera, implemented by the Board, as amended from time to time; and
Valuation Policy	means the valuation policy of Altera, implemented by the Board, as amended from time to time.

Unless a contrary indication appears, any reference in this Policy to:

- (a) any **Policy, Annex** or any other document or instrument, includes (without prejudice to any prohibition on amendments) all amendments and restatements thereof;
- (b) an **amendment** includes a supplement, novation, restatement, or re-enactment and the word **amend** and its derivatives will be construed accordingly;
- (c) an **Annex, paragraph** or **Part** shall, subject to any contrary indication, be construed as a reference to an annex, paragraph or part of this Policy;
- (d) **including** shall not be construed restrictively but shall mean **including but without limitation or prejudice to the generality of the foregoing** and the word **include** and its derivatives will be construed accordingly;
- (e) a **person** shall be construed so as to include its successors in title, permitted assigns and permitted transferees;
- (f) **person** includes any individual, firm, company, corporation, government, state or agency of a state or any association, trust, partnership or other entity (whether or not having separate legal personality) or two or more of the foregoing;
- (g) a provision of law (including EU directives) or regulation (including EU regulations) is a reference to that provision as amended or re-enacted.

Part, paragraph and Annex headings are for ease of reference only.

Annexes form an integral part of this Policy.

In this Policy, words and expressions importing the singular shall, where the context permits or requires, include the plural and vice versa and words and expressions importing the masculine shall, where the context permits or requires, include the feminine and neuter and vice versa.

CODE OF CONDUCT (ANNEX III-IX)

ANNEX III

CONFIDENTIAL INFORMATION

General

- 59 Due to the activities of Altera, personnel will likely have access to inside information or to other sensitive information, such as non-public information concerning investors, investment, or concerning the business of Altera. Employees must exercise due care in the handling of this sensitive information and must keep all such information strictly confidential.
- 60 Without prejudice to the generality of the foregoing, Altera staff shall not on the basis of such sensitive information:
- (i) advise or induce, other than in the proper course of its employment or contract for services, any other person to enter into a transaction;
 - (ii) disclose, other than in the normal course of his employment or contract for services, any information or opinion to any other person.
- 61 In addition, Altera staff is prohibited – and undertakes as such in its employment contract – from disclosing to third parties, in any way whatsoever, any information of which the employee has taken cognizance in the context of the performance of the duties within Altera of which the confidential nature is or should have been familiar to the employee, pertaining to, among others but not limited to, Altera’s business, investors in Altera, and (potential) investments of Altera.

Specific procedures regarding Public to Private Transactions and Public Investments

- 62 Documents regarding public to private transactions and public investments should only be shared within a restricted group of people.

Specific procedures regarding information received from companies

- 63 Personnel 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 may result in a claim for damages against Altera. In addition to potentially being a criminal offense (e.g., a violation of insider trading laws), disclosing confidential information is also a serious breach of trust and can adversely affect our relationships and reputation.

ANNEX IV

CLEAN DESK

Objective

- 64 The objective of this policy is to help to protect Altera against:
- (i) disruption of proper operations;
 - (ii) harm to the reputation of Altera;
 - (iii) financial damage due to abuse or improper use of information; and
 - (iv) loss, theft and undesirable disclosure or damage to information and data carriers.
- 65 This policy on Clean Desks details a number of standards which must be observed by employees when handling information and data carriers. Compliance with this policy will help to prevent damage to the integrity and the reputation of Altera and its employees.

Workplace

- 66 Every employee is personally responsible for the way in which she / he handles information and data carriers. The employee must always handle the entrusted information and data carriers so that only authorized persons have access to this information and data carriers. After working hours, each employee must take reasonable steps to store confidential information and data carriers in a secure place. In addition, the employee should store his personal belongings both during working hours and after working hours in a secure place. Altera is not responsible for the loss or theft of employees' personal belongings.

Department

- 67 After meetings all materials should be removed, discarded or erased from the conference room or other meeting location. This includes overhead sheets, flip-over sheets and writing on whiteboards. The meeting organizer is responsible for ensuring that all materials are removed, discarded or erased.

Computer

- 68 When leaving the office the employee should shut down or log-off her / his computer. If applications are active which cannot be shut down if it would disturb the application's process, the employee shall lock the computer's operating system (e.g., Windows). The employee shall furthermore lock her / his computer when stepping away from his computer.
- 69 The employee shall not prevent the operating system in any way from automatically locking the computer after a certain idle time or from updating its software.

Use of passwords

- 70 The use of other employees' usernames or passwords is not permitted. An employee is prohibited from sharing his/her username or password with others.

Software

- 71 Removing or installing hardware, software or other equipment on the network by individual employees is not allowed without the permission of the ICT department or the designated representative of the ICT department. Employees are not allowed to download software or to otherwise install it. All software must be authorized in advance by the ICT department or the designated representative of the ICT department. Altera has installed virus scanning software on each computer. Employees are not permitted to turn off this virus scanner software or modify its settings. Altera has installed an automatic screensaver on each computer. Employees are not permitted to turn off this screensaver or modify its settings. The employee must ensure that confidential information is stored in a proper way (with due observance of the rules and regulations with respect to processing of personal data). When in doubt on software and data protection the employee must contact the ICT department or the designated representative of the ICT department.

Working at home/use of a private computer

- 72 If confidential company information is taken or used outside of the office by an employee, the employee must ensure that this information is treated carefully and confidentially. The employee is not allowed to store confidential company information on a private computer.

Portable computers/laptops

- 73 The ICT department or the designated representative of the ICT department must ensure that recent anti-virus software is installed on portable computers/laptops. Users of portable computers/laptops must always ensure that information they use is protected. Therefore password protected screensavers and, in case of highly sensitive documents, password protected document protection should be used. The portable computer/laptop must always be transported as hand luggage. A portable computer/laptop should never be left unattended (e.g., a computer/laptop in a car).

ANNEX V

USE OF EMAIL, SOCIAL MEDIA AND INTERNET

Having regard to:

- Section 7:611 and 7:660 of the Dutch Civil Code
- The General Data Protection Regulation

Whereas:

- A. Altera and its employees are bound to treat each other within the spirit of a good employer-employee relationship (Section 7:611 of the Dutch Civil Code).
- B. (Many of) Altera's employees need to use internet and email to perform their work properly.
- C. Social media, such as LinkedIn, provide employees with an opportunity to demonstrate involvement with their work and make a positive contribution to Altera's image.
- D. A code of conduct on the use of email, internet and social media is required given the potential risks involved.
- E. Against the background of these risks, employees are expected to use internet, email and social media in a responsible manner.
- F. Altera is authorised to issue instructions on the use of internet, email and social media and to take measures to ensure the smooth running of the enterprise (Section 7:660 of the Dutch Civil Code).
- G. This code of conduct contains instructions and measures as referred to above.
- H. Altera is authorised to monitor, where necessary, social media use and the use of the email and internet system provided by Altera in order to ensure compliance with this code of conduct.
- I. When performing such monitoring, Altera will observe the fundamental rights and freedoms of the employee(s) involved, in particular the right to privacy.

Has adopted the following code of conduct:

1 Scope

- 1.1** This code of conduct contains instructions on the use of the email and internet system provided by Altera. This code of conduct also contains instructions on both work-related and private use of social media that can impact Altera.

- 1.2** This code of conduct contains instructions on how Altera registers, collects and monitors data and data which can be traced back to an individual with respect to the use of social media and the email and internet system provided by Altera.
- 1.3** This code of conduct applies to all fully or partially automated processing of employee personal data.
- 1.4** This code of conduct applies to all Altera employees. All employees are expected to be familiar with the content of this code of conduct. In this context, the term 'employees' is understood to mean:
- employees with an employment contract
 - members of the Supervisory Board
 - employees with a work placement agreement
 - employees on assignment or secondment
 - hired-in employees and contractors (such as temporary workers, persons employed through a payrolling company, freelance contractors and seconded employees)
 - teleworkers
 - consultants.

2 Objective

- 2.1** The object of this code of conduct is to promote the responsible use of social media (both private and work-related) and of the internet and email system provided by Altera and to ensure that any monitoring of this use is consistent with the protection of employee privacy.
- 2.2** The aim of any monitoring of personal data regarding the use of social media and the email and internet system provided by Altera is as follows:
- coaching/individual assessment of employees
 - collecting evidence and saving relevant facts
 - ensuring Altera's good reputation is preserved and preventing negative publicity
 - countering improper use such as for harassment, including sexual harassment, and discrimination
 - ensuring company secrets are protected/monitored
 - guaranteeing that Altera's computer equipment and software operate properly
 - supervising cost and capacity management.
- 2.3** Email messages may be monitored for one of the following purposes:
- to ensure business continuity in the event of the absence, illness or dismissal of the employee

- to resolve ICT problems (with the employee's consent)
- to ensure business continuity in the event of emergency situations.

3 General principles

- 3.1** Altera supports an open dialogue, the exchange of ideas and the sharing of knowledge through the use of social media and the email and internet system provided by Altera. Altera reminds its employees of their own responsibility.
- 3.2** Altera reserves the right to monitor where necessary its employees with respect to the use of social media and the email and internet system provided by Altera. Any monitoring will take place in accordance with Article 8 of this code of conduct.
- 3.3** This code of conduct has been drawn up in conformity with the General Data Protection Regulation.
- 3.4** Personal data will only be used for the purpose for which they have been collected (see Article 2 of this code of conduct).
- 3.5** Data concerning the use of social media and the email and internet system provided by Altera that can be traced to an individual will not be registered, collected, checked, combined or processed other than in the manner agreed to in this code of conduct. Situations that are not provided for in this code of conduct will be handled in accordance with the labour law framework and the General Data Protection Regulation.
- 3.6** Personal data on the use of social media and the email and internet system provided by Altera will not be retained longer than necessary, with a minimum retention period of 1 month, unless there is a legitimate interest that necessitates the extension of this period.
- 3.7** The employer will take measures regarding the position and integrity of the system administrator (DHS) and the monitoring thereof.
- 3.8** The system administrator is permitted, provided the management's consent has been obtained, to make personal data of users temporarily inaccessible should essential work make this unavoidable. Other than in acute emergency situations, the employees involved will be informed of this temporary inaccessibility.

4 Risks

- 4.1** Failure to adhere strictly to the code of conduct can result in the following risks:
- unauthorised persons gaining access to confidential data;
 - unauthorised persons copying, changing, destroying and/or adding data;
 - unauthorised use or installation of software;

- overburdening of a computer's network or memory;
- increased susceptibility of the communication platform to viruses and malware;
- the spread of information that is discriminatory, sexually intimidating or threatening in nature.

4.2 The possible consequences of these risks are as follows:

- loss of information;
- unintentional disclosure of confidential or sensitive information;
- stagnation or cessation of company processes;
- violation of software licensing agreements;
- copyright violation;
- substantial financial loss;
- negative publicity for the employer;
- pressure on the working relationship between employees.

5 Email use

5.1 Employees are to use Altera's email system for business purposes.

5.2 Employees are entitled to briefly use the email system for non-work-related purposes for sending and receiving both internal and external personal email messages, provided such use does not disrupt or impair the progress and quality of the employee's daily tasks, is not disruptive to others and does not adversely affect the network's operation.

5.3 The general standards of decency apply to work-related email use.

5.4 Employees are not permitted to use the email system to send messages with pornographic, racist, discriminatory, insulting or offensive content.

5.5 Employees are not permitted to use the email system to send messages with content that is harassing/sexually harassing.

5.6 Employees are prohibited from using the email system to send messages that could incite hate and/or violence.

5.7 It is prohibited to distribute chain letters, spam and viruses or to burden the email system in any other way that would result in the network being unduly burdened and/or the proper conduct of the enterprise's affairs being disrupted.

5.8 In the interest of preventing spam, employees are not permitted to leave their Altera email addresses on the internet, unless this is for work-related purposes.

6 Internet use

6.1 Employees are to use Altera's internet system for business purposes. Consequently, its use is related to the performance of employee's duties.

- 6.2 Employees are entitled to briefly use the internet system for non-work-related purposes, provided such use does not disrupt or impair the progress and quality of the employee's daily tasks, is not disruptive to others and does not adversely affect the network's operation.
- 6.3 The general standards of decency apply to work-related internet use.
- 6.4 Employees are not permitted to use the internet system to download and save files for their own private use.
- 6.5 Employees are not permitted to use the internet system to deliberately visit websites containing pornographic, racist, discriminatory, insulting or offensive material or which have a criminal background or intent (e.g. related to hacking). Employees are prohibited from downloading such material.
- 6.6 Employees are not permitted to deliberately visit gambling websites.
- 6.7 Employees are prohibited from engaging in internet use that is unlawful or which constitutes an offence. All legal prohibitions apply at Altera. For example, it is prohibited to use the internet system to download or distribute images, programmes and music files illegally.
- 6.8 Employees are not permitted to seek unauthorised access to non-public sources via the internet system.

7 Work-related social media

- 7.1 Only those authorised employees designated by the management (hereinafter "authorised employee(s)") are permitted to be active on work-related social media, such as Altera's LinkedIn page, on behalf of Altera as part of their job duties.
- 7.2 The authorised employees are permitted to share knowledge and standard company information via the work-related social media in accordance with the instructions provided.
- 7.3 The authorised employees are to remain within their own areas of expertise. If in doubt, the authorised employee must contact the Management Board.
- 7.4 The authorised employees are not permitted to publish confidential information and/or company-sensitive information of Altera on the work-related social media (unless permission has been obtained from Altera's Management Board or Altera's Investor Relations) or to make negative comments, in whichever manner, about Altera and/or its employees.
- 7.5 The authorised employees are not permitted to publish confidential and/or damaging information with respect to the business associates of Altera (e.g. shareholders, and/or customers, and/or lessees and/or property managers and/or other parties with which

AlterA has a business relationship) on work-related social media, unless prior permission has been obtained from the Management Board or Investor Relations.

- 7.6 The authorised employees who publish messages on the work-related social media that can be related to AlterA must in principle state their organisation and job title.

Private social media use

- 7.7 AlterA employees may be active on their private social media for private purposes, provided such use does not impair the productivity of AlterA employees or damage AlterA's image.
- 7.8 Employees are not permitted to publish work-related subjects on their personal social media (this does not include publication of AlterA's general information and the position/job title of the employee at the company or the publication of work-related subjects on personal social media that have already been posted on AlterA's social media by the authorised employee, such as the sharing of a message that has been posted on AlterA's LinkedIn page or website).
- 7.9 In the interest of preventing damage to AlterA's image, employees are not permitted to express themselves negatively on their personal social media about their employer AlterA and/or its employees and AlterA's direct business associates.
- 7.10 Employees must be aware that they bear a responsibility in their private use of social media and that private opinions can easily be confused with AlterA's official point of view. They must be fully aware that everyone can read what they write.

Social media (general)

- 7.11 Employees are personally responsible for the content that they publish on social media.
- 7.12 Employees must be aware of their relationship with AlterA. They must ensure that their social media use is in accordance with general standards of decency.
- 7.13 Employees must be aware that published content will remain in the public domain indefinitely, also after that content has been deleted. This can have consequences for AlterA's image.
- 7.14 Employees must take account of image rights, copyright and the right to quote.
- 7.15 In the event of the slightest doubt whether a publication violates this code of conduct or contains any information that could reflect negatively on AlterA, the employee must contact the Management Board or the department/employee responsible.
- 7.16 An employee must be the first person to correct their own mistakes, without first editing or deleting previous messages. When doing so, the employee must state that they are the person that has edited the message.

8 Monitoring

- 8.1 The possible monitoring of the use of social media and the email and internet system provided by Altera constitutes a processing of personal data within the meaning of the General Data Protection Regulation.
- 8.2 Monitoring of the use of social media and the email and internet system provided by Altera will only take place if such monitoring is deemed necessary within the context of the objectives referred to in Article 2.
- 8.3 In principle, monitoring takes place at the level of totalised traffic data that cannot be traced to identifiable individuals.
- 8.4 If an employee or group of employees is suspected of having violated the rules of this code of conduct, more intensive, targeted monitoring (of content) may take place for a set (short) period of time.
- 8.5 Prior to the targeted monitoring (of content), the employer will inform the employee(s) concerned of 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 9 of this code of conduct.
- 8.6 On an incidental basis, the employer may covertly monitor an employee without first informing the employee concerned, but only if there is a compelling reason for doing so.
- 8.7 Data of anyone who is able to invoke statutory privilege on grounds of the confidential nature of their position will not be monitored.

9 Rights of the employee

- 9.1 *Right of inspection:* Employees have the right to inspect recorded data that relates to them. Requests for inspection will be granted within 20 business days.
- 9.2 *Right to obtain copies:* Employees have the right to obtain copies of any recorded data that relates to them within 20 business days.
- 9.3 *Right to correction:* Employees have the right to correct or supplement, personally or through a third party, factually incorrect information in the recorded data. Decisions on requests to correct or supplement will be taken within 20 business days. If a request to correct or supplement is granted, the correction will be made immediately.
- 9.4 *Right to erasure:* Employees have the right to delete and destroy recorded data that relates to them which is either irrelevant or no longer relevant, factually incorrect or in contravention of this code of conduct or a statutory provision. Decisions on requests to delete and destroy recorded data will be taken within 20 business days. If such a

request is granted, the recorded data concerned will be deleted and destroyed immediately.

10 Penalties

- 10.1** In the event of actions in violation of this code of conduct, the company interests or the generally accepted standards for using social media and the email and internet system provided by Altera, measures may be taken depending on the nature and seriousness of the violation.
- 10.2** For employees, such measures mean disciplinary measures and measures under employment law, such as a reprimand, transfer, suspension or termination of the employment agreement.
- 10.3** For guests, such measures could be temporary or permanent denial of access to the network or internet.

11 Final provision

- a. Altera's Management Board is authorised to amend or revoke this code of conduct.
- b. Employees who can use Altera's email and internet facilities and who have access to social media also sign this code of conduct to demonstrate that they are aware that they are bound by it. If the code of conduct is amended, they will need to sign the amended version.

ANNEX VI

MIXING PRIVATE AND BUSINESS INTERESTS AND PERSONAL INVESTMENT

11.1 DOEL

Doel van deze gedragscode is het waarborgen en handhaven van het vertrouwen in Altera Vastgoed NV door belanghebbenden, door gewenst gedrag te stimuleren en ongewenst gedrag te voorkomen. De gedragscode geeft regels en richtlijnen voor de in paragraaf 1.3 van deze code omschreven doelgroep ter voorkoming van conflicten tussen belangen van de vennootschap en de privébelangen van betrokkenen, alsmede ter voorkoming van het gebruik maken van vertrouwelijke informatie van de vennootschap voor privédoeleinden.

Het uitgangspunt daarbij is om transparantie te bevorderen en ervoor te zorgen dat alle betrokkenen, ook voor hun eigen bescherming, duidelijk weten wat wel en wat niet geoorloofd is. In de arbeidsvoorwaarden van de medewerkers van Altera Vastgoed NV zijn reeds enkele bepalingen opgenomen. De bepalingen van de gedragscode Altera Vastgoed NV zijn een specifieke aanvulling daarop en een nadere uitwerking daarvan.

De gedragscode beoogt mede bij te dragen tot het integer functioneren van Altera Vastgoed NV ten behoeve van al diegenen die bij de vennootschap belang hebben en tot het waarborgen van de goede naam en reputatie van de vennootschap.

De directie van de vennootschap is verantwoordelijk voor het naleven van de verplichtingen die voortvloeien uit enige wettelijke bepaling of enige bepaling uit de gedragscode.

11.2 NORMEN

Van iedere betrokkene wordt verwacht dat hij/zij zich integer gedraagt (zorgvuldig, uitlegbaar en standvastig handelt) en hij/zij zich onder alle omstandigheden zal gedragen volgens de hoogste normen van de bedrijfsethiek. Dit betekent onder meer dat alle betrokkenen moeten voorkomen dat hun privébelangen in conflict komen c.q. verstrengeld raken met de belangen van de vennootschap, dan wel dat de schijn wordt gewekt dat zulks het geval kan zijn. Dit geldt bij alle contacten met derden.

11.3 DOELGROEP

Deze gedragscode is van toepassing op de Raad van Commissarissen, de directie, alle andere medewerkers van de vennootschap, en eventueel door de directie als zodanig aangewezen personen, allen tezamen hierna te noemen “betrokkene(n)”.

Met betrekking tot directie en alle medewerkers van de vennootschap, hierna te noemen “insider(s)”, gelden in aanvulling op de algemene bepalingen van hoofdstuk 1 verdergaande voorschriften dan voor de overige. Deze verdergaande voorschriften zijn opgenomen in hoofdstuk 2 van deze gedragscode.

Zowel het direct als indirect overtreden van de regels van de gedragscode is niet toegestaan. Daarom is het de betrokkene niet toegestaan derden te betrekken bij handelingen die in strijd zijn met de gedragscode. Onder “derden” worden in deze gedragscode steeds mede verstaan echtgenoten, partners, gezins- en familieleden en huisgenoten.

11.4 COMPLIANCE OFFICER

Voor de werkzaamheden voortvloeiend uit de gedragscode, het integriteitsbeleid, de klokkenluidersregeling en de incidentenregeling wordt de compliance functie uitgevoerd door de Compliance Officer bij Altera Vastgoed NV (thans per 1/1/2020 mw. mr. R. Smaal).

11.5 VERTROUWELIJKHEID

De betrokkene mag geen vertrouwelijke informatie over de zaken in het algemeen betreffende de vennootschap, alsmede over beleggingen die hem in de loop van zijn dienstverband ter kennis zijn gekomen anders dan ten behoeve van en in het belang van de vennootschap, aan derden bekend maken of door achteloosheid aan anderen bekend te laten worden.

Evenmin mag de vertrouwelijke informatie ten eigen voordele of ten behoeve van anderen gebruikt worden, dan wel een poging hiertoe worden verricht. Onder vertrouwelijke informatie wordt verstaan informatie die niet publiek toegankelijk is.

Bovendien zijn de betrokkenen gehouden om strikte geheimhouding te betrachten ten aanzien van de persoonsgegevens van derden waartoe de betrokkene voor zijn/haar werk toegang heeft.

11.6 AANVAARDEN VAN RELATIEGESCHENKEN, UITNODIGINGEN, NEVENFUNCTIES EN HET DEELNEMEN IN ANDERE ONDERNEMINGEN EN INSTELLINGEN

Daar waar goedkeuring in dit hoofdstuk vooraf redelijkerwijs niet mogelijk is, wordt zo spoedig mogelijk achteraf gemeld.

1.6.1 Aanvaarden van relatiegeschenken, uitnodigingen e.d.

Betrokkenen dienen te voorkomen dat ze in een situatie geraken waarin het accepteren van een relatiegeschenk of uitnodiging voor (enige vorm van) entertainment aangeboden door een zakelijke relatie of (mogelijke) aspirant-relatie hun beslissingen kan beïnvloeden. Het is niet toegestaan dat ook maar de schijn van beïnvloedingsmogelijkheid wordt gewekt.

Daarom dienen betrokkenen voorzichtig en terughoudend om te gaan met het aanvaarden van relatiegeschenken en uitnodigingen en deze te melden. Ook pogingen van (aspirant-) relaties tot oneigenlijke beïnvloeding dienen onmiddellijk te worden gemeld. Zie voorts hoofdstuk 3 voor melding en goedkeuring.

1.6.2 Nevenfuncties

Het is niet toegestaan, behoudens goedkeuring (zie hoofdstuk 3), nevenfuncties zoals commissariaten, adviseurschappen, lidmaatschap van beleggingscommissies e.d. te vervullen bij bedrijven en instellingen waarmee de vennootschap zakelijke contacten heeft. Ook het aanvaarden van nevenfuncties bij andere bedrijven en instellingen is onderworpen aan goedkeuring (zie hoofdstuk 3). Bij de afweging of goedkeuring zal worden verleend, zal als leidraad dienen of er sprake is van nevenfuncties welke de schijn hebben of kunnen opwekken van een conflicterend belang met de functie van de betrokkene binnen de vennootschap.

Nevenfuncties samenhangend met een investering of deelneming van de vennootschap waarin de betrokkene uit hoofde van zijn functie formeel is benoemd dan wel voorgedragen en waarbij volledig duidelijk is op grond waarvan betrokkene namens de vennootschap deze nevenfunctie vervult, vallen niet onder het hiervoor vermelde verbod.

1.6.3 Financiële belangen in zakelijke relaties

Betrokkenen mogen geen financiële belangen hebben in een bedrijf of instelling, waarmee de vennootschap zaken doet, of waarschijnlijk zal gaan doen.

1.6.4 (Sub-fonds)leveranciers/aannemers e.d. Altera Vastgoed NV

Gebruik voor privéwerkzaamheden van leveranciers, aannemers, makelaars in onroerend goed, onderhoudsdiensten en/of ander zakelijke dienstverleners waarmee de vennootschap zakelijke contacten onderhoudt is niet toegestaan, behoudens goedkeuring na melding (zie hoofdstuk 3).

Goedkeuring zal alleen verleend worden indien geen alternatieven mogelijk zijn, geldelijk privévoordeel is uitgesloten en de werkzaamheden tegen marktconforme condities worden verricht, ten bewijze waarvan aan de Compliance Officer een kopie van de offerte en de factuur dient te worden overlegd.

1.6.5 Eigendommen Altera Vastgoed NV

Zonder voorafgaande toestemming van de Financieel directeur is gebruik van eigendommen (van het fonds en van de sub-fondsen) van de vennootschap ten eigen bate niet toegestaan. Voorbeelden hiervan zijn kantoorbenodigdheden, computers, computerprogramma's en intellectueel eigendom. Het intellectuele eigendom van specifieke, door de vennootschap ontwikkelde en niet openbaar gemaakte beleggingsinstrumenten of analysemodellen dient overeenkomstig behandeld te worden. Gebruik voor eigen doeleinden of openbaarmaking ervan naar derden is niet toegestaan zonder voorafgaande toestemming van de Financieel directeur.

1.6.6 Waarde en melding van relatiegeschenken

Het in ontvangst nemen van relatiegeschenken, bijvoorbeeld ter gelegenheid van de jaarwisseling, dient beperkt te blijven tot kleine attenties die de commerciële waarden van ongeveer € 75,- (per relatie per jaar) niet te boven gaan en hoeven niet gemeld te worden. Boven € 75,- (per relatie per jaar) dient dit gemeld te worden. Zie hoofdstuk 3 voor melding en goedkeuring. De directie kan besluiten het relatiegeschenk te laten terugsturen.

1.6.7 Geven van relatiegeschenken

Relatiegeschenken aan derden worden nimmer gegeven, behalve voor zover de commerciële waarde de € 75,- (per relatie per jaar) niet te boven gaat.

1.6.8 Uitnodigingen

Uitnodigingen voor reizen, seminars, bedrijfsbezoeken en andere bijeenkomsten in Nederland of het buitenland worden slechts aanvaard na goedkeuring (zie hoofdstuk 3 voor melding en goedkeuring). Teneinde de onafhankelijkheid ten opzichte van derden te waarborgen zijn de reis- en overnachtingskosten van de medewerker steeds voor rekening van de vennootschap, tenzij na melding en goedkeuring (zie hoofdstuk 3) anders wordt bepaald.

1.6.9 Acceptatie

Een uitnodiging kan nimmer worden aanvaard indien er een potentieel belangenconflict is en/of het zakelijke karakter, dan wel het belang van de uitnodiging voor de vennootschap niet kan worden aangetoond.

Het is eveneens niet toegestaan om geld, goederen of diensten in welke vorm dan ook te accepteren van derden, behoudens het in de paragrafen 1.6.6 en 1.6.8 bepaalde.

Zie hoofdstuk 3 voor melding en goedkeuring.

Voorbeelden van hetgeen ongeoorloofd is :

- reizen (vliegtickets, treinkaartjes, passagebiljetten voor reizen per schip, hotel-, appartement- of vakantieverblijf, huurauto's);
- kostenvergoedingen voor partners;
- leveranties van goederen of diensten met ongebruikelijke hoge kortingen of tegen niet-marktconforme tarieven;
- leningen van zakelijk relaties e.d.

1.7 VOORWETENSCHAP

De betrokkene mag niet zakelijk noch privé handelen in financiële instrumenten terwijl hij ter zake beschikt over voorwetenschap. De volgende transacties zijn vrijgesteld van melding en toezicht:

- transacties in obligaties uitgegeven door de Staat en andere overheden;
- transacties in financiële instrumenten waarvan het beheer, op grond van een schriftelijke overeenkomst is overgedragen aan een professionele

vermogensbeheerder, op zodanige voorwaarden dat de insider geen invloed kan uitoefenen op de fondsselectie of op afzonderlijke transacties;

- transacties in indexfondsen of in ter beurze genoteerde rechten van deelneming in (semi)open-ended beleggingsinstellingen, mits de insider binnen die instelling geen functie vervult.

Onder handelen wordt verstaan kopen en verkopen, alsmede het intekenen op emissies van financiële instrumenten.

Onder financieel instrument worden begrepen:

- effect;
- geldmarktinstrument;
- recht van deelneming in een beleggingsinstelling, niet zijnde een effect,
- derivatencontract, waaronder begrepen maar daartoe niet beperkt een optie, future, swap, valuta- en rentetermijncontract;
- overige financiële instrumenten in de zin van de Wet op het financieel toezicht;
- en voorts al hetgeen naar de opvattingen in het maatschappelijk verkeer als zodanig wordt beschouwd.

1.8 MELDING VAN (POTENTIËLE) BELANGENCONFLICTEN

Betrokkene is verplicht elk (potentieel) belangenconflict te melden aan de Compliance Officer. Indien de betrokkene twijfelt over de toepasselijkheid van de gedragscode of de uitleg ervan dient hij de Compliance Officer te raadplegen. Indien het (potentieel) belangenconflict een van de directieleden of een lid van de Raad van Commissarissen betreft, dient deze dit te melden aan de voorzitter van de Raad van Commissarissen van Altera Vastgoed NV en aan de Compliance Officer. In het geval het de voorzitter van de Raad van Commissarissen betreft, wordt het gemeld aan de collega commissarissen en aan de Compliance Officer.

1.9 ONDERTEKENING EN JAARLIJKSE VERKLARING VAN NALEVING

Ieder die in dienst treedt van Altera Vastgoed NV, dan wel op andere wijze toetreedt tot de kring van betrokkenen ontvangt de gedragscode en dient een verklaring van naleving van de gedragscode te ondertekenen.

Elke betrokkene dient vervolgens een verklaring omtrent de naleving van de gedragscode te ondertekenen aan het begin van ieder jaar. Bij tussentijdse indiensttreding zal de betrokkene

de code dienen te tekenen en geldt de verplichting voor de rest van het lopend jaar. De ondertekende verklaring van de naleving van de code wordt jaarlijks verstrekt aan de Compliance Officer.

1.10 SANCTIES

Afhankelijk van de zwaarte van de overtreding wordt de betrokkene gewaarschuwd, dan wel wordt aan de (lijn)directeur van betrokkene geadviseerd deze te schorsen of uit zijn functie bij de vennootschap te ontheffen dan wel andere disciplinaire maatregelen te nemen. De aard van de te treffen sanctie wordt bepaald door de directie tezamen met de voorzitter van de Raad van Commissarissen. Betreft het een directeur dan wordt de sanctie bepaald door de voorzitter van de Raad van Commissarissen en de Raad van Commissarissen. Betreft het de voorzitter of een lid van de Raad van Commissarissen, dan zal melding worden gedaan aan de collega commissarissen en vervolgens aan de aandeelhouders. De Algemene Vergadering van Aandeelhouders beslist over een eventuele sanctie.

2. BEPALINGEN VOOR ALTERA VASTGOED NV INSIDERS

2.1 ZAKELIJKE RELATIES

Een insider is een aan de vennootschap verbonden persoon, die direct of indirect bij transacties van de vennootschap is betrokken, dan wel anderszins uit hoofde van zijn/haar werkzaamheden, beroep of functie over voorwetenschap beschikt of kan beschikken. Een insider is ook de verbonden persoon die kan beschikken over andere vertrouwelijke (markt)informatie.

Het is de insider niet toegestaan privétransacties te verrichten met of door tussenkomst van natuurlijke personen met wie de insider een zakelijke relatie onderhoudt. Onder privétransacties worden hier in ieder geval mede begrepen het handelen in financiële instrumenten.

2.2 INDIRECTE TRANSACTIES

Het hierboven onder punt 2.1 gestelde is, onder verwijzing naar het onder punt 1.3 vermelde, van toepassing, ongeacht of de insider handelt (rechtstreeks of indirect via deelnemingen, beheerders of andere derden met uitzondering van “vrije hand”-transacties)

- voor zichzelf dan wel namens anderen;

- alleen of in samenwerking met anderen;
- en bewust of onbewust met voorwetenschap waar vanuit gegaan kan worden dat hij hierover beschikt.

2.3 PRIVE-VASTGOEDTRANSACTIES

De insider is verplicht om onverwijld (voorgenomen) persoonlijke vastgoedtransacties schriftelijk (per mail volstaat) aan de Compliance Officer te melden en de Compliance Officer legt dit schriftelijk vast.

3 MELDING EN GOEDKEURING

Melding en verkrijgen van goedkeuring is een verantwoordelijkheid van een ieder individu verbonden aan de vennootschap. De Compliance Officer treedt daarbij ook op als adviseur voor zover daar behoefte aan is, en als administrateur in het licht van de monitoringsactiviteiten die voortvloeien uit het toezicht op de naleving van de gedragscode. De Compliance Officer ontvangt direct een kopie van de vastlegging van meldingen ten behoeve van de controle op de naleving van de gedragscode (mail volstaat).

Indien op grond van het hiervoor gemelde een meldingsplicht ontstaat of goedkeuring moet worden gevraagd, dan geldt de volgende procedure:

3.1 MELDING AAN DE COMPLIANCE OFFICER (EN FINANCIËEL DIRECTEUR)

- De betrokkene meldt en/of vraagt schriftelijke goedkeuring aan de Compliance Officer ingeval van alle hiervoor genoemde meldingen, tenzij een het uitnodiging of geschenk betreft zoals genoemd in paragraaf 1.6.6 (“Waarde en melding geschenken”) of paragraaf 1.6.8 (“Uitnodigingen”) betreft (zie hiervoor onder 3.2.).
- Vervolgens meldt de Compliance Officer alle gedane meldingen en/of vraagt de Compliance Officer goedkeuring van alle gedane verzoeken aan de directie en legt dit schriftelijk vast.
- Iedere betrokkene is verplicht elk (potentieel) tegenstrijdig belang of reputatierisico onmiddellijk te melden aan de Financieel directeur en de Compliance Officer. Pogingen van een (aspirant-) relatie tot beïnvloeding dienen eveneens overeenkomstig bovenstaande onmiddellijk te worden gemeld.

3.2 MELDING AAN DE EIGEN LEIDINGGEVENDE EN (LIJN) DIRECTEUR

- De betrokkene vraagt schriftelijke goedkeuring (per mail volstaat) aan de eigen leidinggevende en/of zijn/haar (lijn)directeur van een geschenk met een waarde van meer dan € 75,- (zoals genoemd in paragraaf 1.6.6.) of een uitnodiging (zoals genoemd in paragraaf 1.6.8.)
- Na schriftelijke goedkeuring (per mail volstaat) van de hierboven genoemden registreert betrokkene dit zelf op de “geschenken-/uitnodigingenlijst” die op een algemeen bekende toegankelijke plek beschikbaar is gesteld (Intranet of E:schijf).
- Betrokkene stelt de Compliance Officer schriftelijk in kennis van de melding en goedkeuring (per mail volstaat).
- Bij twijfel over melding of goedkeuring wordt de Compliance Officer om advies gevraagd.
- De “geschenken-/uitnodigingenlijst” wordt periodiek in het directieoverleg besproken.

4. GEGEVENS BEWAREN EN GEHEIMHOUDING

De meldings- en/of goedkeuringsgegevens van de betrokkene worden maximaal vijf jaar bewaard. De Compliance Officer en de directieleden zijn gehouden tot geheimhouding van de informatie verstrekt door betrokkenen of derden (uitgezonderd meldingen over geschenken en uitnodigingen die op een algemeen toegankelijke lijst worden gezet).

5. ONVOORZIENE OMSTANDIGHEDEN

Over kwesties waarin deze gedragscode niet voorziet, beslist de directie.

ANNEX VII

CLUSTER MUNITION

Altera shall not:

- (i) execute transactions, or have transactions executed on its behalf, with the aim to acquire or offer a financial instrument which is issued by: a Cluster Munition Company involved in the production, sale or distribution of cluster munition (as described in Article 2 of The Convention on Cluster Munitions adopted on May 30, 2008 in Dublin) or crucial elements thereof or an undertaking which owns more than 50% of the share capital of a Cluster Munition Company;
- (ii) provide loans to a company referred to under (i); or
- (iii) acquire non-freely transferable participation in the capital of a company referred to under (i).

This prohibition does not apply to: (a) transactions based on an index which for less than 5% consists of companies referred to under (i), (b) transactions in funds managed by third parties which for less than 5% consist of companies referred to under (i), and (c) investments in well-defined projects of companies referred to under (i), to the extent the financing will not be used for production, sale or distribution of cluster munition.

ANNEX VIII

COMPLIANCE POLICIES AND PROCEDURES ACKNOWLEDGEMENT FORM

I, [NAME EMPLOYEE], hereby acknowledge that I have received, diligently read and understand the following policies applicable within Altera Vastgoed N.V. (**Altera**):

- (a) the Compliance Policy;
- (b) the Conflict of Interest Policy;
- (c) the Remuneration Policy;
- (d) the Risk Management Policy;
- (e) the Transparency Policy;
- (f) the Service Provider Policy;
- (g) the Valuation Policy;
- (h) the AML/KYC Policy;
- (i) Product approval and review process Policy; and
- (j) the AO/IC Guide,

(the **Policies**).

In addition, I agree with the importance of compliance of these Policies and will therefore ensure compliance with the Policies during my tenure with Altera as well as thereafter to the extent such is explicitly provided for in the relevant Policies. This statement does not prejudice any restrictive covenant under or arising pursuant to any (employment or management) agreement entered into between myself and Altera.

On [DATE], in [LOCATION], this form was made by [NAME]:

Signature [NAME]

ANNEX IX

INCIDENT NOTIFICATION FORM

Name and role of person completing this form:

Signature of person completing this form:

Date:

Incident

Date and time of incident²:

Name/s of person/s involved in the incident:

characteristics of incident:

Witnesses (include contact details):

² Incidents are irregularities which are or can be a serious danger for the integrity of Altera, and may be the result of the conduct of:

- a) an employee or a member of the Board of Altera;
- b) a shareholder of Altera; or
- c) a person or an entity performing activities for or on behalf of Altera.

These irregularities may include: breaches of laws and legislation, breaches of Policies, fraud, corruption, and other undesirable behavior.

Reporting of the incident to superior

Incident Reported to:	Date:
How (this form, in person, email, phone):	

Measures taken in response to the incident

Description of actions to be taken:

On [DATE], in [LOCATION], this form was made by [NAME]:

Signature [NAME]
