Incidents Regulations

Altera Vastgoed NV

Adopted in the Management Team meeting on 24 May 2018

Background and purpose

Altera Vastgoed N.V. (to be referred to further as: 'Altera') views the good reputation and integrity of its organization as a crucial requirement for operating successfully as a real estate investment institution. Despite all the efforts taken, incidents or unfortunate events may arise. This may happen at Altera itself or at one of its Contractors. Altera's reputation may also be jeopardized in these situations.

The purpose of these Incidents Regulations is to make clear to interested parties how incidents will be reported, recorded and investigated and how these will be the basis for taking corrective measures. The idea is not only to correct the specific situation that has occurred, but also to learn from the situation.

Distinction between Incident and Wrongdoing

Altera's Integrity Policy describes the overarching policy on restrained, ethical business operations. The Integrity Policy describes which separate sets of regulations have further shaped this policy. These Incidents Regulations are one of these underlying policy documents.

An 'Incident' is conduct or an event which seriously threatens the Company's ethical running of its business. An Incident can take many forms, such as an operational Incident, a gross violation of the laws or regulations (Wrongdoing), or a security Incident. Other types of Incidents are conceivable, too. The cause may be either internal or external.

An Incident needs to be handled in conformity with the Incidents Regulations.

In the case of Wrongdoing or irregularities, there has been abuse of a position of power or knowledge or other position, or violation of internal or external rules, by one or more individuals. Gross Wrongdoing, however, may also constitute an Incident if such Wrongdoing seriously threatens the ethical running of the business.

Wrongdoing or irregularities must be handled in conformity with the Whistleblower Regulations.

If an associated person is unsure whether Wrongdoing, irregularities or an Incident is involved, he/she can always contact the Confidential Advisor beforehand, so as to select the most appropriate course of action.

1. Definitions

1.1 Incident:
Conduct or an event that seriously threatens Altera's ethical running of its business.

An Incident can take many forms, such as an operational Incident, a gross violation of the laws or regulations (Wrongdoing), or a security Incident. Other forms of Incidents are conceivable, too. The cause may be either internal or external.

An Incident will be characterized as a serious Incident if:
a. the Incident seriously threatens Altera's ethical running of its business;
b. there is a high risk that Altera's image will be harmed in the media;
c. the Incident has a major effect on the operations;
d. the Dutch Public Prosecution Service [*Openbaar Ministerie*] has become involved in the matter;
e. the Incident relates to fraud;
f. a designation order has been issued by the regulatory authority or an order subject to a penalty for non-compliance has been given, or the imposition of an administrative fine has been proposed.

1.2 Data Leak (see Appendix: Data Leaks Procedure):
A breach of security as referred to in Articles 4(12), 33 and 34 of the General Data Protection Regulation (GDPR)[1], in which personal data has been exposed to loss or unlawful processing, hence, to risks against which protective measures (Article 5 GDPR) should have offered protection.

[1] " 'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

1.3 Reporting Party:
Anyone who reports an Incident in connection with these Regulations. This may be persons associated[2] with Altera or Contractors' or other interested parties' employees.

1.4 Contact Point:
The Company's Data Protection Officer will be the contact point for Data Leaks. For other Incidents, the Contact Point will be the CEO or, if the Reporting Party suspects that Management Board members are involved, the Company's Supervisory Board chairperson or the Confidential Advisor.

1.5 Contractor:
Any third party, whether a natural person or legal entity, performing work directly or indirectly for, on behalf of or for the benefit of Altera at Altera's request. This may also include Contractors processing personal data for Altera ('Processors').

2. General

2.1 Altera's Management Board will be responsible for handling Incidents in a timely, efficient manner, recording these and taking appropriate corrective measures.

2.2 The Company's Management Board will ensure that all of Altera's associated persons are aware of and the Contractors' and other interested parties' relevant workers can access the Incidents Regulations through the Altera website.

3. Reporting Incidents

3.1 Every associated person must report an Incident or a suspected Incident immediately to the Contact Point. Reports may be made verbally or in writing.

3.2 Other interested parties with knowledge of or suspicions about an Incident are encouraged to bring this to Altera's attention immediately.

3.3 The Reporting Party and the external compliance officer will get written confirmation that the report has been received.

3.4 The external compliance officer will record reports of Incidents in the Incidents Register on the date of receipt. During the rest of the process, relevant documents will be placed in the file, such as the communications between the various relevant parties, the reporting on the process, and the results of any investigation.

4. The investigation

4.1 The Contact Point will discuss a report that has been received with the Management Board. The Contact Point will advise the Management Board to set aside the report if an initial analysis indicates that there is no basis for the report.

4.2 If the Incident pertains to a Contractor's operations, Altera and the Contractor will work together as much as possible in dealing with the Incident.

4.3 If the initial analysis provides serious indications of a potential Incident, the Management Board will have the report investigated further. The Management Board will assess whether a separate investigative committee will be established or whether it itself will lead the investigation. If there is a suspicion that a Management Board member is involved, the Supervisory Board will be informed immediately, and the Supervisory Board will then lead the investigation, too. The external compliance officer will be informed simultaneously.

4.4 If the report concerns a Data Leak, the Data Leaks Procedure will apply (see Appendix). Any other Incidents will be further handled in conformity with these Incidents Regulations.

4.5 The Reporting Party will be informed that an investigation will be initiated. The manner of investigation and the period within which the investigation must be completed will depend on the nature of the Incident.

4.6 The Management Board will monitor the progress of the investigation.

[2] See Altera's Code of Conduct for the definition of 'relevant parties'.

4.7 If people are investigated during the investigation, the provisions in the privacy laws will be complied with in full.

4.8 The Management Board will decide which consequences, if any, will be attached to the results of the investigation, after having informed the Supervisory Board about this.

5. Investigations of serious Incidents

5.1 Supplementary to Article 4, the Management Board will, If the report concerns a serious Incident, regularly report to the Supervisory Board and the external compliance officer on the progress of the handling of the report.

5.2 The CEO will decide on the communications, both internal and external, regarding serious Incidents. The Management Board will determine whether, in which order and at which time the following parties must be informed and will receive advice in this respect from the external compliance officer and the Supervisory Board.

a. the external accountant;
b. the custodian;
c. the shareholders;
d. the regulatory authority (the Dutch Authority for the Financial Markets [*Autoriteit Financiële Markten*] (AFM));
e. the press;
f. the Public Prosecution Service/police.

6. Results of investigation

6.1 The results of the investigation will be reported by the Management Board to the Supervisory Board and the external compliance officer. This report will include a brief account of the facts and circumstances, the evidence in general terms, any time-critical or other report to the regulatory authorities and the advice on the measures to be taken.

7. Measures

7.1 Based on the investigation results, the Management Board will assess and decide on any adjustment of the procedures and other measures to correct the operations.

7.2 If the Incident occurred at a Contractor, the Contractor itself will be responsible for the measures to be taken. Altera will be consulted and informed by the Contractor about the measures to be taken and the progress.

7.3 Causing or otherwise being involved in an Incident may result in job-related sanctions, including summary dismissal. If there have been wilful violations amounting to serious criminal offences, such as the crimes mentioned in the Dutch Criminal Code [*Wetboek van Strafrecht*] and Economic Offences Act [*Wet op de economische delicten*], a report will be filed with the law enforcement officials or police in principle.

7.4 The external compliance officer will, on management's behalf, monitor the implementation of and compliance with new procedures and measures effectuated in response to the Incident.

8. Recording of reports

8.1 In an Incidents Register, the Contact Point will record all reports received, the facts and circumstances, follow-up actions, investigations initiated, investigation results, preventive and repressive measures taken, and the reports to the regulatory authorities. Systematic recording of reports will be designed in part to clarify Incidents, so similar situations can be avoided.

9. Reporting

9.1 The Contact Point will report on the Incidents in the regular annual reporting in such a way that confidentiality remains adequately safeguarded.

10. External report

10.1 The Management Board may file a report with law enforcement officials in connection with the Incident.

10.2 Where applicable, the Management Board will, in consultation with the external compliance officer, file a report with the relevant regulatory authorities. If an Incident pertains to a Contractor, this partner will be consulted as well. The report will consist of the relevant facts and circumstances of the Incident and the measures taken or to be taken in response to the Incident. The most important regulatory authorities in this context are the AFM and the Dutch Data Protection Authority [*Autoriteit Persoonsgegevens*].

11. Protection

11.1 The Reporting Party will not experience any adverse consequences in any sense whatsoever if the report was made in good faith.

11.2 Any person receiving information about an Incident (or report of an Incident) by virtue of these Regulations will treat this as strictly confidential with respect to third parties, unless, under these Regulations or under or pursuant to the law, the power or obligation exists to furnish this information to third parties.

12. Final provision

The Management Board may amend these Incidents Regulations. These Incidents Regulations will take effect on 24 May 2018.

Signature

Amstelveen, the Netherlands, 24 May 2018

The Management Board of Altera Vastgoed NV

Appendix

Data Leaks Procedure

Effective 25 May 2018, the Dutch Personal Data Protection Act [*Wet bescherming persoonsgegevens*] (PDPA), along with the Dutch Data Breaches (Reporting Obligation) Act [*Wet meldplicht datalekken*], was replaced with the General Data Protection Regulation (GDPR). The Data Breaches (Reporting Obligation) Act has been anchored in the GDPR since 25 May 2018, and this means that Altera must immediately report Data Leaks to:

- the Dutch Data Protection Authority [*Autoriteit Persoonsgegevens*] (Dutch DPA) (Article 33 GDPR);
- in certain cases, the Data Subjects (Article 34 GDPR).

This Procedure describes the actions to be taken within Altera if:

- there is a Data Leak or a Data Leak is suspected within Altera;
- there is a Data Leak at one of Altera's Contractors (for example, a real estate manager or the payroll bureau, that is, Altera's Processors, and/or Altera's other Contractors, that is, an estate agent, developer or building contractor).

This Procedure is based in part on Working Party 29's policy rules (European Guidelines on Personal Data Breach Notification). See the link: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=61205.

For each reported Data Leak, Altera will retain the freedom to assess whether this Procedure must be followed or whether deviating from the Procedure is justifiable.

1. Definitions
Besides the definitions from the Incidents Regulations, the following definitions will apply in the Data Leaks Procedure.

Dutch DPA:
The Dutch Data Protection Authority.

GDPR:
The General Data Protection Regulation (in effect since 25 May 2018).

Data Subject:
A natural person to whom Personal Data relates (Article 4(1) GDPR).

Security Incident[3]:
A breach of security (as referred to in Article 33(1) GDPR) in which the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (for instance, the Personal Data has not been exposed to loss or unlawful processing); this does not constitute a Data Leak.

Data Leak[4]:
A breach of security (as referred to in Articles 33(1) and 34 GDPR) in which the personal data breach is likely to result in a risk to the rights and freedoms of natural persons (for instance, the Personal Data has been exposed to loss or unlawful processing); this does constitute a Data Leak.

Contact Point:
The Company's Data Protection Officer, and, in his/her absence, Altera's CFO, will be the contact point for Data Leaks.

Personal Data:
Any information concerning an identified or identifiable natural person. This includes nearly everything about the person, from the IP address, name and address, e-mail address, telephone number, vehicle registration number,

[3] Always let the Contact Point be the one to determine whether there has been a Security Incident or Data Leak (say, because of a wrongly sent e-mail, stolen phone or lost document). And report this immediately!
[4] Always let the Contact Point be the one to determine whether there has been a Security Incident or Data Leak (say, because of a wrongly sent e-mail, stolen phone or lost document). And report this immediately!

and photograph to the identification number, location data and anything which says something about a natural person. (Article 4(1) GDPR).

Processor (Articles 4(8) and 28 GDPR):
The Contractor processing Personal Data for Altera, without being subject to its direct authority. The purpose of and means for the data processing are determined by the Controller. The Processor does not take any decisions on the use of the data, providing it to third parties or other recipients, the period for which the data will be stored, and so on. If the Processor does gain such control, it must be considered a Controller (as referred to in Articles 4(7) and 24 GDPR).

Controller (Articles 4(7) and 24 GDPR):
The party determining, alone or together with others, the purpose of and means for processing Personal Data (Article 4(7) GDPR).

Processing of Personal Data:
Any act or aggregate of acts regarding Personal Data, including in any event compiling, recording, classifying, saving, updating, modifying, requesting, consulting, using, furnishing (through forwarding) or disseminating data or any other form of providing or assembling data or relating data to each other, as well as protecting, erasing or destroying data (Article 4(2) GDPR).

PDPA:
The Dutch Personal Data Protection Act.

2. Identification of Data Leak
Anyone who suspects[5] or observes a Data Leak must inform the Contact Point at Altera without any unnecessary delay, but in any event within 48 hours of discovery.

The Reporting Party will provide information about:
a. all of the facts and circumstances regarding the observation or suspicion;
b. upon request, additional information which the Contact Point needs to initiate any investigation and to make a report to the regulatory authority.

These agreements have been agreed on in writing with Contractors processing Personal Data for Altera ('Processors'). Besides the aforementioned information, the Contractor will furnish information about the measures that the Contractor has already taken or proposes to take to limit and remedy the adverse consequences from the breach.

3. Assessment of Data Leak (yes/no)
Based on the information obtained, and if a Data Leak is suspected, the Management Board and the Data Protection Officer will jointly assess as soon as possible whether a Data Leak has actually occurred. The external compliance officer may furnish advice in this regard.

The assessment whether there has been an Incident that must be reported to the Dutch DPA will be made using the diagrams found in Working Party 29's policy rules (European Guidelines on Personal Data Breach Notification; http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=61205).

An assessment will also be made as to whether measures must be taken immediately to limit damage, including providing a provisional or other report to Data Subjects.

If the Incident has not resulted in the loss or unlawful Processing of Personal Data, a Data Leak has not occurred, but instead a Security Incident. Reporting to the Dutch DPA will be unnecessary in that case. The Management Board will, however, consult with the Data Protection Officer on whether it makes sense to investigate the security leak to prevent a recurrence. The external compliance officer will be informed of the result and the considerations leading to the decision.

4. Report to the Dutch DPA (Article 33 GDPR)
After coordination with the Management Board, the Data Protection Officer will ensure that an electronic report is filed with the Dutch DPA in a timely manner (immediately, without any unnecessary delay and, if possible, no later than 72 hours after the Data Leak is discovered) and in accordance with the Dutch DPA's online report form. The Data Protection Officer will act as the contact person for communications with the Dutch DPA. This will also be the case if it is not clear yet whether the Incident represents a Data Leak.

If the specific situation lends itself to this, the Management Board will ask the Contractor to make the report with the Dutch DPA and to keep the Management Board and Data Protection Officer apprised of the report.[6]

5. Assessment as to whether Data Leak should be reported to Data Subjects (Article 34 GDPR)
Together with the Data Protection Officer, the Management Board will determine whether the Data Leak must be reported as well to the persons whose data it concerns. The European Guidelines on Personal Data Breach Notification (http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=61205) will likewise be used here.

The external compliance officer may furnish advice in this regard.

6. Causes and corrective measures at the Contractor
The Contractor at which the Data Leak arose must, in observing the Data Leak, take, at its own expense and risk and in consultation with Altera, any necessary measures to stop the Data Leak and limit the damage that ensues or may ensue from this. The Contractor will fully inform Altera and keep it fully informed of the developments concerning the Data Leak and the measures taken or to be taken to limit the consequences and prevent a recurrence.

[5] At all times, the principle here is that it is better for an employee of Altera or the Contractor to make a report which turns out to have been unnecessary than to decide not to report this to the Contact Point in case of doubt. The Contact Point will make this assessment.
[6] This clause applies only to Contractors or other third parties which are not Processors for Altera.

Based on the information received, the Management Board will assess whether it is necessary to ask the Contractor to take certain additional security measures. The Management Board will monitor the progress of any additional security measures.

7. Recording of reports

Altera's Contact Point will record all reports received, the facts and circumstances, follow-up actions, investigations initiated, investigation results, preventive and repressive measures taken, and the reports to the regulatory authority. Systematic recording of reports will be designed in part to clarify Incidents, so similar situations can be avoided. Every Incident and Data Leak will be recorded in the Processing Register (Article 30 GDPR).

The Contractor will also keep such a register of any Data Leaks observed or suspected at it.