Altera Management B.V.

C3. Incident Policy

1 April 2025

This Policy including the Annexes is adopted by the Management Board of Altera in April 2025.

AlterA Creating sustainable value

Version management

Determination date	April 2025
Version	2.2
Review date	October 2026
Author	Frank Stockmann
Logfile/changes	July 2024: The following sections have been amended in the Incident Regulations: 4. General, 5 Examples of (possible) incidents, 6 Prioritisation of incidents, 10 supervisor and 16 Awareness & protection. Changes that have been made within the Data Breach procedure are as follows: 1 Considerations, 6 Cooperation with the provision of data in relation to the Data Breach, 7 Availability of personnel after discovery of Data Breach, 9 Consequences of reporting Data Breaches and 12 Reporting reports. October 2024: Processing the comments and adjustments of the members of the Management Board and adding DORA requirements. April 2025: Processing the comments and adjustments of the members of the Management Board and adding DORA requirements. Plus some typos improved.

Contents

1 Background and purpose

Altera Management B.V. (hereinafter "Altera"), in its capacity as manager, 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, considers the good reputation and integrity of its organisation to be a crucial condition for the successful operation of a real estate investment fund manager. Despite all the efforts made, incidents can occur. This can be done at Altera itself or at one of its Contractors. Altera's reputation and integrity may also be jeopardised by these behaviours or events.

The purpose of this policy is to make it clear to stakeholders how Incidents will be reported, recorded and investigated and how they will be the basis for taking corrective action. The idea is not only to correct the specific incident that occurred, but also to learn from the incident.

2 Distinction between Incident and Wrongdoing

Altera's Code of Conduct describes the overarching policy for controlled and ethical business operations. The Code of Conduct describes which individual regulations have further shaped this policy. This policy is one of these underlying policy documents.

An 'Incident' is a behaviour or event that poses or may pose a serious threat to Altera's ethical business operations. An Incident can take many forms, such as an operational Incident, a gross violation of the law or regulation (Abuse) or a Security Incident. Other types of incidents are also conceivable. The cause can be both internal and external.

An Incident must be handled in accordance with this policy.

In the case of Abuses or irregularities, there is abuse of a position of power or knowledge or other position, or violation of internal or external rules, by one or more persons. However, gross violations can also constitute an Incident if such violations seriously threaten ethical business operations.

Wrongdoing or irregularities must be dealt with in accordance with the Whistleblower Policy.

If an employee is not sure whether there is a wrongdoing, irregularity or Incident, he/she can always contact the confidential adviser in advance to choose the most appropriate course of action.

3 Definitions

1. Incident
Conduct or event that poses or may pose a serious threat to Altera's ethical business operations.

An Incident can take many forms, such as an operational Incident, a gross violation of the law or regulation (Abuse) or a Security Incident. Other forms of incidents are also conceivable. The cause can be both internal and external.

A behaviour or event is considered an Incident in the following situations.
- it poses a serious threat to Altera's ethical business operations;
- there is a great risk that Altera's image will be damaged in the media;
- it has a major impact on business operations;
- the Public Prosecution Service has started to get involved in the case;
- it relates to fraud;
- the regulatory authority has issued a designation order or imposed an order subject to a penalty for non-compliance, or an administrative fine has been proposed.

2. Data Breaches (see Appendix III: Data Breach Procedure)
A breach of security as referred to in Article 4(12), and Articles 33 and 34 of the General Data Protection Regulation (GDPR),[1] whereby personal data is exposed to loss or unlawful processing, and therefore to risks against which protective measures (Article 5 GDPR) should have provided protection.

3. Reporting party
These may be persons associated with[2] Altera or Contractors or other interested parties who are obliged to report an Incident in connection with these Terms and Conditions immediately.

4. Point
The company's Privacy Officer will be the point of contact for data breaches. For other Incidents, the point of contact is the Compliance Officer. If the Reporter suspects that the Compliance Officer is the cause of the Incident, the Reporter will inform the members of the Management Board or the confidential advisor.

5. Contractor
Any third party, natural or legal person, who, at the request of Altera, directly or indirectly performs work for, on behalf of or for the benefit of Altera. These may also be Contractors who process personal data for Altera ("Processors").

6. Confidential advisor:
The person selected by Altera's management to provide information on how to tackle undesirable behaviour and to advise Altera's management on the prevention of undesirable behaviour.

7. Code of conduct
This is one of the pillars of ethical business operations within Altera.

---

[1] "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
[2] See Altera's Code of Conduct for the definition of 'relevant parties'.

8. Whistleblower Regulations
Internal rules within Altera to ensure a safe and honest environment for all people who work at and for Altera.

9. Customer
Participants and tenants.

10. Board/Management
Altera's Management Board consists of the Chief Executive Officer, Chief Financial Officer and Chief Investment Officer. They are responsible for the day-to-day management and represent Altera externally.

11. Incident Register
The register in which Incidents are registered by the Compliance Officer.

4 General

1. The Management Board of Altera is responsible for the timely and efficient handling of Incidents, recording them and taking appropriate corrective measures.
2. Altera's management ensures that all persons associated with Altera are aware of the most recent Incident Regulations and that the relevant employees of the Contractors and other interested parties have access to the most recent Incident Regulations via the Altera website.

5 Internal Incident Reporting

1. Each employee must immediately report an Incident or a suspected Incident to the Point of Contact by completing the Incident Notification Form of Appendix II – Incident Notification Form or otherwise in writing.
2. Other interested parties (such as contractors) with knowledge of or suspicions about an Incident are encouraged to bring this to the attention of Altera immediately.
3. The Reporter and the Compliance Officer will receive written confirmation that the report has been received.
4. The Compliance Officer records reports of Incidents in the Incident Register on the date of receipt. During the rest of the process, relevant documents are placed in the file, such as the communication between the various relevant parties, the report on the process and the results of a possible investigation.
5. The structure and categories of external mandatory regulations have been taken into account when setting up the incident reports at Altera.
6. In the run-up to the monthly risk & compliance meeting (with the participation of the CFO, Head of Control, the Compliance Officer and the Risk Manager), the Compliance Officer and the Risk Manager check the event register for the presence of Incidents.

6 Research

1. The Contact Point discusses a report received with the Management Board. The Contact Point advises the Management Board to set aside the report if an initial analysis shows that there is no basis for the report.
2. If the Incident relates to the business operations of a Contractor, Altera and the Contractor will cooperate as much as possible in handling the Incident.
3. If the initial analysis provides serious indications of a possible incident based on the incident prioritisation matrices of Part 2 in Appendix I – Incident Judgment, the Management Board will have the report further investigated. The Management Board will assess whether a separate investigation committee will be set up or whether it will lead the investigation itself. If there is a suspicion that one or more of the members of the Management Board are involved, the Supervisory Board leads the investigation and vice versa.
4. If the notification relates to a Data Breach, the Data Breach Procedure applies (see Appendix III – Data Breach Procedure). Any other Incidents will continue to be dealt with in accordance with these Incident Regulations.
5. The Reporter is informed that an investigation will be initiated. The method of investigation and the period within which the investigation must be completed depends on the nature of the Incident.
6. The Management Board monitors the progress of the investigation.
7. If an investigation is carried out into persons during the investigation, the provisions of the privacy legislation will be fully complied with.
8. The Management Board will decide what consequences, if any, will be attached to the results of the investigation before informing the Supervisory Board thereof.

7 Communication of Incidents

1. If the report concerns a critical or high (1 or 2) according to the Incident prioritisation matrix of Appendix I part 2.4) Incident, the Management Board shall regularly report to the Supervisory Board and the Compliance Officer on the progress of the handling of the report. Other Incidents (medium, low and very low) are only reported to the Supervisory Board and the Compliance Officer if the Management Board sees reason to do so.
2. The Management Board decides on communication, both internal and external, in relation to an Incident. The Management Board determines whether, in what order and at what time the following parties must be informed and receives advice from the Compliance Officer and the Supervisory Board:
   a. external auditor;
   b. keeper;
   c. Participants;
   d. supervisor (the *Netherlands Authority for the Financial Markets* (AFM) and *the Dutch Central Bank* (DNB));
   e. the press;
   f. Public Prosecutor's Office/police/FIU.

8 Reporting Incidents to the regulatory authority

Pursuant to Section 4:11(4) of the Financial Supervision Act, Incidents related to the following subjects must always be provided to the Netherlands Authority for the Financial Markets:

1. Conflict of interest;
2. Violations of the law and other violations that may damage confidence in Altera and/or in the financial markets;
3. Impairment of clients' confidence in Altera and/or the financial markets;
4. Critical or high (1 or 2) ICT Incidents according to the Incident prioritisation matrix of Appendix I part 2.4;
5. Critical or high (1 or 2) cyber threats, according to the Incident prioritisation matrix of Appendix I part 2.4., only if the Management Board sees reason to report it;
6. Other acts or behaviour of Altera or its employees that impair the integrity, control or transparency of business operations.

Incidents that are classified as 1, 2 or 3 according to Annex I, section 2.5 must also be reported to the Netherlands Authority for the Financial Markets.

9 Reporting DORA ICT Incidents to the regulatory authority

In accordance with Article 19 of the DORA Regulation and Articles 20a and 20b of the RTS/ITS for Incidents, Altera must report ICT Incidents to the Netherlands Authority for the Financial Markets in accordance with the procedure set out below.

From the moment the ICT Incident is classified as critical or high (1 or 2) according to the Incident prioritisation matrix of Appendix I part 2.4, a first report must be shared with the Authority within 4 hours from the moment the ICT Incident is classified as critical or high, this may not be longer than 24 hours after the ICT Incident has been detected.

- First notification → In the first notification, Altera records general information about the ICT Incident, such as the description of the ICT Incident, when the ICT Incident was detected and the qualification of the ICT Incident. At that time, Altera also states how the ICT Incident was discovered, whether the ICT Incident occurs more often and what the cause of the ICT Incident is. If possible, Altera will also provide an indication of whether the business continuity plan has been activated as a result of the ICT Incident and whether the ICT Incident has had an impact on other financial institutions and third parties.
- Interim report → The interim report must be submitted to the Dutch Data Protection Authority within 72 hours of the classification of the ICT Incident. In this phase, too, Altera is obliged to report when the ICT Incident was identified and on the basis of which criteria it was classified. It also describes the type of ICT Incident in combination with the affected business departments, such as business processors and infrastructure components. It will also be clarified whether the ICT Incident has been communicated to the clients and what temporary measures have been taken to recover from the ICT Incident. In this phase, the consequences are also shared by Altera, analysing whether vulnerabilities have been exploited and whether there are signs that the IT systems or IT infrastructure can no longer be used safely.

- Final report → Within one month of classification of the ICT Incident, a final report of the ICT Incident must be shared with the Authority. If the ICT Incident has not been resolved by that time, the final report will be submitted no later than one day after the ICT Incident has been definitively resolved. The final report contains the date on which the ICT Incident was resolved, information about the cause of the ICT Incident and information about Altera's inability to comply with legal requirements and contractual agreements/SLAs (if applicable). The final report also describes the actions taken by Altera to resolve the ICT Incident and prevent a recurrence of the ICT Incident. In addition, Altera will provide information on the direct and indirect costs incurred as a result of the ICT Incident.

10 Reporting DORA Significant Cyber Threats to the Regulatory Authority

In accordance with Article 19 of the DORA Regulation and Articles 20a and 20b of the RTS/ITS for Incidents, Altera has the option of voluntarily reporting cyber threats to the Netherlands Authority for the Financial Markets in accordance with the procedure set out below.

- When Altera informs the Authority, Altera ensures that the following points are taken into account:
  - The date on which the cyber threat was identified;
  - A description of the cyber threat;
  - The current status of the cyber threat;
  - The potential impact of the threat on Altera;
  - What measures have been taken to prevent the threat from becoming a reality;
  - In the case of customers, participants or other business relations, it is confirmed whether they have been informed of the appropriate protective measures they can take.

As of 17 January 2025, Altera and other financial institutions that are required to comply with DORA and are subject to the AFM regime will have the opportunity to report cyber threats and ICT Incidents in an online environment of the AFM.

11 Results of the study

The results of the investigation will be reported by the Management Board to the Supervisory Board and the Compliance Officer. This report contains a brief explanation of the facts and circumstances, the evidence in general terms, any report to the supervisors that is critical of time or otherwise, and the advice on the measures to be taken.

12 Measures

1. Based on the results of the investigation, the Management Board will assess and decide on any adjustment of the procedures and other measures to correct the operations.
2. If the Incident has occurred at a Contractor's premises, the Contractor is 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.
3. Causing or otherwise being involved in an Incident may result in employment-related sanctions, including instant dismissal. In the event of intentional violations that constitute serious criminal offenses, such as the crimes referred to in the Criminal Code and the Economic Offences Act, a report is in principle made to the enforcers or police.
4. The Compliance Officer will supervise the implementation and compliance with new procedures and measures implemented in response to the Incident on behalf of the Management Board.

13 Registration of reports

In the Incident Register, the Compliance Officer records all reports received, the facts and circumstances, follow-up actions, investigations initiated, investigation results, preventive and repressive measures taken and the reports to the supervisors. Systematic registration of reports is partly intended to provide insight into incidents, so that similar behaviour or events can be prevented in the future.

14 Reporting

The Contact Point reports on the Incidents in the regular annual reporting in such a way that confidentiality is sufficiently guaranteed.

15 External report

The Management may submit a report to law enforcement officials in connection with the Incident. Where appropriate, the Management Board, in consultation with the Compliance Officer, will submit a report to the relevant regulatory authorities. If an Incident relates to a Contractor, this party will also be consulted. The report will consist of the relevant facts and circumstances of the Incident and the measures that have been or must be taken as a result of the Incident. The most important supervisory authorities in this regard are the AFM and the Dutch Data Protection Authority.

16 Awareness and protection

1. To lower the threshold for employees to report events, the Compliance Officer gives an annual awareness presentation about the importance of reporting incidents.
2. The Reporter will not suffer any adverse consequences, in any way whatsoever, if the report is made in good faith.

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

Annex I : Assessment of Incidents

1 Examples of (possible) Incidents

In the letter of 23 December 2022, the AFM provided a number of examples of (possible) Incidents, divided into the topics (i) information security Incidents and (ii) integrity Incidents. This has been supplemented with Incidents criteria of the DORA scheme.

(i) Information Security Incidents:
1. Theft or loss of ICT resources containing confidential data from Altera.
2. Unauthorised access to Altera's ICT infrastructure, possibly resulting in unauthorised transactions.
3. The installation of malware on Altera's systems.
4. A data breach, in which confidential information has ended up in the public domain.
5. DDoS attacks or the threat thereof.
6. Relevant data (such as name, address, place of residence, bank account number and/or BSN) loss of a significant number of clients due to the actions of Altera or those of its Contractors.
7. ICT Incidents with an impact on our critical ICT business functions.
8. ICT Incidents with a lower impact, but which have occurred more often (more than twice) over a three-month period and have the same cause and similar impact.
9. Cyber threats that can be classified as significant due to the threat to our critical business processors.
10. Cyber threats with a high probability of manifestation.

(ii) Integrity incidents:
1. An employee, policymaker or Contractor who is suspected of and/or prosecuted for a criminal (economic) offence.
2. A member of the Management Board or member of the Supervisory Board who has been fined (in the past) for intentionally filing an incorrect or incomplete tax return.
3. An employee or Contractor who has stolen money from Altera and/or its Clients.
4. If Altera is fined by the regulator (AFM) or another (foreign) regulator than the AFM.
5. If a Client or a contractor of Altera has become involved in serious (economic) unlawful acts.

2 Incident Prioritisation

2.1 Prioritising incidents

To make it easier to take the right measures for the Incident, it is important to prioritise Incidents. The prioritisation of Incidents is based on two factors: **urgency and impact.** The priority of an Incident is determined by the assessment of its impact and urgency, where:
- Urgency is the measure of how quickly the Incident needs to be resolved.
- Impact is the measure of the extent of the Incident and of the potential damage resulting from the Incident before it can be resolved.

Under Incidents with an * are DORA-related ICT Incidents or cyber threats.

Altera strives to comply with the following principles of 2.2 - 2.5. if the Incident was caused by Altera. Service Level Agreements relating to the follow-up of Incidents are leading if Incidents are not caused by Altera.

2.2 Urgency of Incidents

Category Urgency	Description
High (H)	• The damage caused by the Incident is increasing rapidly. • Work that needs to be repaired by staff and/or contractors is very labour-intensive. • The Incident results in a significant risk of serious adverse consequences, but has serious adverse consequences for the protection of personal data.
Average (M)	• The damage caused by the Incident increases significantly over time. • Work is lost, but can be recouped relatively quickly.
Low (L)	• The damage caused by the Incident increases only slightly over time. • The work that remains is not time-consuming.

2.3 Impact of the Incident

Category Urgency	Description

High (H)	• Critical services have been affected where malicious unauthorised access to network and information systems has been identified and may have resulted in data loss.*
	• A relatively large number of employees have been affected by the Incident and/or are no longer able to perform their work. Several departments have been affected.
	• More than 25% of the Clients are affected and/or suffer damage in any way as a result of the Incident. Their personal data has been compromised.
	• More than 25% of the Clients are affected and/or suffer damage in any way as a result of the Incident. Their personal data has been compromised.*
	• More than 30% of all contractors used are affected.*
	• This is more than 10% of the daily average number of transactions.*
	• The financial impact of the Incident for Altera is more than € 100,000.
	• Costs and losses of Altera amount or are likely to exceed € 100,000 (may be based on estimates where actual values cannot be determined).*
	• The Incident results in a significant risk of serious adverse consequences, but has serious adverse consequences for the protection of personal data. When assessing the impact of the Data Breach, the following is important:
	  • the nature and extent of the Data Breach;
	  • the nature of the personal data breached;
	  • the extent to which technical protection measures have been taken;
	  • the consequences for the privacy of the data subjects.
	• There is reputational damage, negative national media attention.
	• Any impact on the availability, authenticity, integrity or confidentiality of data that has or will have a negative impact on the implementation of Altera's business objectives or on compliance with legal requirements.*

	• Any impact on reputation, as evidenced by any of the following:*
	  • Incident reflected in the media; or*
	  • Received repeated complaints; or*
	  • Inability to comply with regulatory requirements; or*
	  • Likely loss of customers or participants with a material impact on Altera's business.* The duration of the incident is greater than 24 hours or the downtime of the service is greater than 2 hours for the ICT services that support critical or important functions.*
	  • Any impact of the Incident that has been identified on the territory of at least two countries.*
	  • There are physical injuries.

Average (M)	• Some employees are affected by the Incident and/or can no longer do their job, for example a department. • Between 10% and 25% of the Clients are affected and/or suffer damage in any way as a result of the Incident. Their personal data has been compromised. • The financial impact of the Incident is higher than € 50,000 but less than € 100,000. • There is a risk of reputational damage.
Low (L)	• Some employees have been affected by the Incident and/or are no longer able to do their work. • Less than 10% of the Clients have been hit and/or have suffered damage, but this is very minimal. Personal data has been compromised. • The financial impact of the Incident is less than € 50,000. • There is no chance of reputational damage.

2.4 Incident Prioritisation Classes

The Incident Priority is obtained by comparing urgency and impact. This results in the Incident Priorities Matrix.

		Impact		
		High	**Average**	**Low**
Urgency	High	1	2	3
	Average	2	3	4
	Low	3	4	5

2.5 Incident Priority Matrix

Below are the results worked out with a code and color. Reaction time is the time to respond to the Incident after noticing. Addressing time is the time to inform those involved in the Incident.

Code / color	Description	Responsiveness	Addressing time
1	Critical	Directly	4 hours
2	High	10 minutes	8 hours
3	Average	1 hour	24 hours
4	Low	4 hours	1 week
5	Very low	1 day	2 weeks

Annex II : Incident Notification Form

Name and role of the person filling out this form:
Signature of the person filling out this form:
Date:

Incident

Date and time of the Incident:
Name(s) of the person(s) involved in the Incident:
Features of the Incident:
Witnesses (including contact details):

Reporting the Incident to Supervisor

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

Actions taken in response to the Incident

Description of the actions to be taken:

_____

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

Signature [NAME]

_____

Annex III : Data Breach Procedure

1 Considerations

- Altera attaches great importance to the proper security of its (electronic) systems in which personal data are stored and processed.
- However, it can never be completely prevented that a data breach will occur.
- Under the General Data Protection Regulation (GDPR), Altera is obliged to report Data Breaches to the Dutch Data Protection Authority and to the data subject if the privacy of the data subject is at stake as a result of the Data Breach.
- Altera wishes to comply with its legal obligations.
- Altera has therefore formulated a policy to act as adequately as possible in the unlikely event of a data breach.

2 Data Breaches

As of 25 May 2018, the Personal Data Protection Act (Wbp) and the Data Breach Notification Act have been replaced by the General Data Protection Regulation (GDPR). The Data Breach Notification Act has been enshrined in the GDPR since 25 May 2018, which means that Altera Data Breaches must immediately report to:

- Dutch Data Protection Authority (Article 33 GDPR);
- in certain cases, the data subject (Article 34 GDPR).

This Procedure describes the actions that must be taken within Altera if:

- there is a Data Breach or a Data Breach is suspected within Altera;
- there is a Data Breach at one of Altera's Contractors (for example, a property manager or at Altera's Processors and/or other Altera Contractors, i.e. a broker, developer or contractor).

Altera reserves the right to assess, for each reported Data Breach, whether this Procedure should be followed or whether deviating from the Procedure is justified.

3 Definitions

In addition to the definitions from the Incident Regulations, the following definitions apply in the Data Breach Procedure:
AP: the Dutch Data Protection Authority.

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

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

Security incident[3]: A breach of security (as referred to in Article 33(1) GDPR) where the personal Data Breach is unlikely to pose a risk to the rights and freedoms of natural persons (e.g. the personal data has not been exposed to loss or unlawful processing); this does not constitute a personal Data Breach.

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

Point of contact: The company's Privacy Officer, and in the absence of Altera, Altera's CFO, is the point of contact for data breaches.

Personal Data: Any information relating to an identified or identifiable natural person. This includes almost everything about the person, from the IP address, name and address, email address, telephone number, license plate number and photo to the identification number, location data and everything that says something about a natural person (Art. 4 (1) GDPR).

Processor (Article 4(8) and (28) of the GDPR): The Contractor that processes personal data on behalf of Altera, without this being under its direct authority. The purposes and means of data processing are determined by the controller. The Processor does not make any decisions about the use of the data, its provision to third parties or other recipients, the period for which the data is stored, and so on. If the Processor does acquire such control, it must be regarded as the Controller (as referred to in Article 4 paragraph 7 and Article 24 GDPR).

Controller (Articles 4(7) and 24 of the GDPR): the party that determines, alone or jointly with others, the purposes and means of the processing of personal data (Article 4(7) of the GDPR).

Processing of personal data: any operation or set of operations relating to personal data, including in any case the compilation, recording, classification, storage, adaptation or alteration, retrieval, consultation, use, disclosure (by transmission) or dissemination of data or any other form of provision or compilation of data or the linking of data, as well as the protection, protection and protection of data deletion or destruction of data (Article 4 (2) GDPR).

Wbp: the Personal Data Protection Act.

---

[3] Always let the Point of Contact be the one who determines whether there is a security incident or data breach (e.g. due to a missent email, stolen phone or lost document). And report this immediately!
[4] Always let the Point of Contact be the one who determines whether there is a security incident or data breach (e.g. due to a missent email, stolen phone or lost document). And report this immediately!

4 Identification of a Data Breach

Anyone who[5] suspects or discovers a Data Breach must notify the Contact Point at Altera without delay, or otherwise, but in any case by completing the Data Breach Form of Appendix IV – Data Breach Form within 48 hours of discovery.

The Reporter will provide information about:
a. all facts and circumstances relating to the observation or suspicion;
b. upon request, additional information required by the point of contact to conduct an investigation and report to the regulatory authority.

These agreements have been agreed in writing with Contractors who process Personal Data for Altera ("Processors"). In addition to the aforementioned information, the Contractor will provide information about the measures that the Contractor has already taken or intends to take to limit and remedy the adverse consequences of the infringement.

5 Assessment of a Data Breach

On the basis of the information obtained and if there is a suspicion of a Data Breach, the Management Board and the Privacy Officer will jointly assess whether there has actually been a Data Breach as soon as possible. The Compliance Officer can advise on this.

It will also be assessed whether immediate measures should be taken to limit the damage, including providing a (preliminary) report to those involved.

If the Incident has not resulted in the loss or unlawful processing of personal data, it is not a Data Breach, but a Security Incident. In that case, reporting to the AP is not necessary. However, the Management Board will consult with the Privacy Officer about whether it is useful to investigate the security vulnerability in order to prevent a recurrence.

6 Cooperation in the provision of data in connection with the Data Breach

The discoverer/reporter of the Data Breach offers full cooperation to the internal responsible party by providing answers to the following questions as quickly and as effectively as possible (in writing by filling in the Data Breach Form of Appendix IV – Data Breach Form): Other departments (such as IT) can be called in by the discoverer/reporter to answer the questions.

- What happened? (description of the incident)
- Was it accidental or was it caused by malicious intent (e.g. hacked data)?
- When did it happen? (date and time)
- When was it discovered?
- What types of personal data or data files (registers) were involved in the reported data breach?
- Is the data encrypted, and if so, how?
- Can the data be deleted remotely or made inaccessible, and if so, has that happened?

[5] The basic principle here is at all times that it is better for an employee of Altera or the Contractor to make a report that turns out to have been superfluous than to decide not to report this to the Contact Point in case of doubt. The Contact Point will make this assessment.

- What are the possible consequences for those involved?
- Which group(s) of people are/are affected?
- How many people are (approximately) bothered by this?
- Have data of individuals in other EU countries also been affected by the Data Breach?
- Were technical and/or organisational measures already possible as a result of the Incident?

7 Availability of personnel after discovery of Data Breaches

The person responsible for the department from which the Data Breach took place, as well as the discoverer of the Data Breach and anyone who, from his/her position, can take organisational measures to limit the consequences of the Data Breach, must remain available for consultation with the Contact Point or any experts appointed by him for the work assigned to him if this is necessary as a result of the Data Breach.

8 Notification to the AP (Article 33 GDPR)

After consultation with the Management Board, the Privacy Officer will ensure that the Data Breach is reported electronically to the AP in a timely manner (immediately, without undue delay and, if possible, no later than 72 hours after the Data Breach has been discovered) and in accordance with the AP's online notification form. The Privacy Officer will act as a contact person for communication with the DPA. This will also be the case if it is not yet clear whether the Incident is a Data Breach.

If the specific situation lends itself to this, the Management Board will ask the Contractor to report the report to the AP and to keep the Board and the Privacy Officer informed of the report[6].

9 Consequences of reporting Data Breaches

1. If the Data Breach has negative consequences for the data subjects, the Contact Point will do everything in its power to limit these consequences as much as possible.
2. Depending on the nature and extent of the Data Breach for the data subjects, the reporting point determines:
   - how the data subjects are informed (including in any case the information about the types of personal data affected, what the possible consequences are, what measures Altera takes and how the data subjects can prevent or (limit) the damage themselves);
   - what aftercare the people involved receive;
   - what actions are needed in the interest of the organisation.

3. If a Data Breach has occurred – regardless of whether it has been reported or not – adequate technical and/or organisational measures will be taken as soon as possible to prevent future similar Data Breaches.

[6] This clause only applies to Contractors or other third parties who are not Processors for Altera.

10 Assessment of whether a Data Breach must be reported to the Data Subjects (Article 34 GDPR)

The Management Board, together with the Privacy Officer, determines whether the Data Breach must also be reported to the persons involved.

An external lawyer can advise on this.

11 Causes and corrective measures at the Contractor

If the Contractor with which the Data Breach has occurred, it must take all necessary measures at its own expense and risk and in consultation with Altera to stop the Data Breach and to limit the damage that results or may result from it. The Contractor will fully inform Altera and keep it fully informed of the developments surrounding the Data Breach and the measures taken or to be taken to limit the consequences and prevent a recurrence.

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.

12 Registration of reports

The Altera Contact Point registers all reports received, the facts and circumstances, follow-up actions, investigations initiated, investigation results, preventive and repressive measures taken and the reports to the regulator. The systematic recording of reports will be partly designed to clarify data breaches, so that similar situations can be prevented. Each Data Breach is registered in the Data Breach Register within the Privacy Perfect system and has the following points:

- a description of the Incident;
- date and time of the Data Breach;
- date and time of discovery of the Data Breach;
- description of the type of personal data breach;
- description of the category(ies) of affected persons;
- the approximate number of persons involved;
- whether data of individuals in other EU countries have also been breached;
- whether the Incident has been reported to the Dutch Data Protection Authority and, if so, the date and time of the report;
- whether the Incident has been reported to the data subjects and, if so, the date and time of the report;
- the way in which the data subjects were informed;
- consequences of the Data breach, indicating the date and time if possible; and
- which technical and/or organisational measures have been taken as a result of the Data Breach, stating the date and time.

The Contractor will also keep such a register of all Data Breaches detected or suspected by it.

13 Assessment

This policy is reviewed every two years

Annex IV : Data Breach Form

On	Data Processing Officer (FS) / Privacy Officer (FS)
From	
Number of the extension	.....
Date	-- month year
About	Form Datalek: attn. direct one Datalek to the Privacy Officer (FS) (orally/by e-mail). This form is used to assess whether a Datalek must be reported to the AP within 72 hours.

1. Date of the Data Breach
2. Description of the Data Breach (how, what and to whom)
3. Was it accidental or was it caused by malicious intent (e.g. hacked data)?
4. Which personal data has been breached?
5. What damage can this cause/what adverse consequences will the data subjects whose data has been leaked as a result suffer?
6. Can the data be deleted remotely or made inaccessible, and if so, has that happened?
7. How many people (whose personal data is involved) are involved in the Data Breach?
8. Have data of individuals in other EU countries also been affected by the Data Breach?
9. What can you do to limit the adverse consequences of this Data Breach? *(e.g. withdrawal of email, promise of deletion of the mail by the recipient who received it unintentionally, etc. and if possible attach documents to this form)*
10. Were technical and/or organisational measures already possible as a result of the Incident?
11. What are you going to do/or do you have an idea to prevent such a data breach in the future?
12. Other relevant information

Thanks for filling it in!

Assessment/motivation of whether a Data Breach should be reported to the DPA or to the data subjects (to be completed by DPO/PO)