AlterA

Get into real good

Altera Vastgoed NV

Incident Regulations Policy

This Incident Regulations Policy including its Annexes (the Policy) is adopted by the Management Board of Altera in October 2023

Version management

Determination date	October 2023
Version	2.1
Review date	October 2024
Author	**Frank Stockmann**
Logfile/changes	**27 July:The following parts have been changed in the Incidents Regulations: 4. Generals, 5 Examples of (possible) incidents, 6 incidents prioritization, 10 regulatory authority and 16 awareness & protection. Changes that has been made within the Data Breaches procedure are as followed: 1 Considerations, 6 Cooperation with data provision regarding the data Breach, 7 staff availability after Data Breach discovery, 9 consequences of reporting Data Breaches and 12 reporting of reports. October: Processing the comments and adjustments from the Management Board Members.**

Table of Contents

1. 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 may arise. This may happen at Altera itself or at one of its Contractors. Altera's reputation and integrity may also be jeopardized in these conducts or events.

The purpose of this policy 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 Incident that has occurred, but also to learn from the Incident.

2. Distinction between Incident and Wrongdoing

Altera's Code of Conduct describes the overarching policy on restrained, ethical business operations. The Code of Conduct describes which separate sets of regulations have further shaped this policy. This policy is one of these underlying policy documents.

An 'Incident' is a conduct or an event which (can) 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 this policy.

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.

3. Definitions

1. Incident:

Conduct or an event which (can) seriously threaten 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 conduct or event will be characterised as an 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.

2. Data Breaches (see Appendix III: Data Breaches 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."*

3. Reporting Party:
This may be persons associated[2] with Altera or Contractors' or other interested parties' employees who are obliged to report an Incident in connection with these Regulations immediately.

4. Contact Point:
The Company's Data Protection Officer will be the contact point for Data Breaches. For other Incidents, the Contact Point will be the Compliance Officer or, if the Reporting Party suspects that involved, the Compliance Officer is involved, the Management Board members or the Confidential Advisor will be informed.

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').

6. Confidential Advisor:
The person selected by Altera's management to provide information about tackling undesirable behaviour and advising Altera's executives and management in preventing undesirable behaviour.

7. Code of Conduct:
The overarching policy on restrained, ethical business operations within Altera.

8. Whistleblower Regulations:
Internal rules within Altera to ensure a safe and ethical environment for all persons who work at and for Altera.

9. Client:
Investors and tenants.

10. Management Board:
The executive directors within Altera consisting of the chief executive officer, chief financial officer and chief investment officer. They are responsible for the day-to-day management and represent Altera to the outside world.

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

4. General

1. Altera's Management Board will be responsible for handling Incidents in a timely, efficient manner, recording these and taking appropriate corrective measures.
2. Altera 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 most recent Incident Regulations policy through the Altera website.

5. Reporting Incidents

1. Every employee must report an Incident or a suspected Incident immediately to the Contact Point by filling in the Incident Notification Form of appendix II – Incident Notification Form or otherwise in writen.
2. Other interested parties (such as contractors) with knowledge of or suspicions about an Incident are encouraged to bring this to Altera's attention immediately.
3. The Reporting Party and the Compliance Officer will get written confirmation that the report has been received.
4. The 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.
5. In the run-up to the monthly risk & compliance meeting (attended by the CFO, Head of Control, Reporting Manager, the Compliance Officer and the Risk Manager), the Compliance Officer and the Risk Manager check the events register for the presence of incidents.

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

6. The investigation

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.
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.
3. If the initial analysis provides serious indications of a potential Incident based om the incidents prioritization matrices of section 2 in Appendix I – Incidents Judgement, 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 the CFO or/and the CIO are involved, the CEO will lead the investigation and vice versa.
4. If the report concerns a Data Leak, the Data Breaches Procedure will apply (see Appendix III – Data Breaches procedure). Any other Incidents will be further handled in conformity with these Incident Regulations.
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.
6. The Management Board will monitor the progress of the investigation.
7. If people are investigated during the investigation, the provisions in the privacy laws will be complied within full.
8. The Management Board will decide which consequences, if any, will be attached to the results of the investigation, before informing the Supervisory Board about this.

7. Investigations of Incidents

1. The Management Board will, if the report concerns an Incident, regularly report to the Supervisory Board and the compliance officer on the progress of the handling of the report.
2. The Management Board will decide on the communications, both internal and external, regarding an Incident. 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 compliance officer and the Supervisory Board:

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

8. Regulatory authority

According to article 4:11 fourth paragraph of the AFS, incidents related to below topics must always be provided to the Dutch Authority for the Financial Markets:
1. Conflict of interest;
2. Offenses of the law and other violations that may damage the confidence in Altera and / or in the financial markets;
3. Damage in the confidence of clients regarding Altera and / or the financial markets;
4. Other acts by Altera or the employees that are contrary to the unwritten laws of the society.

The Management Board will also report all Incidents classified as **1, 2 or 3 according to Part 4 of appendix I Incident Judgement** towards the Dutch Authority for the Financial Markets.

9. Results of investigation

1. The results of the investigation will be reported by the Management Board to the Supervisory Board and the 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.

10. Measures

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.
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.
3. Causing or otherwise being involved in an Incident may result in job-related sanctions, including summary dismissal. If there have been willful 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.
4. The compliance officer will, on management's behalf, monitor the implementation of and compliance with new procedures and measures effectuated in response to the Incident.

11. Recording of reports

1. Inthe Incidents Register, the Compliance Officer 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 conducts or events can be avoided.

12. Reporting

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

13. External report

1. The Management Board may file a report with law enforcement officials in connection with the Incident.
   Where applicable, the Management Board will, in consultation with the 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*].

14. Awareness & Protection

1. To lower the threshold for employees to report events, yearly the compliance officer gives an awareness presentation about the importance of reporting Incidents.
2. The Reporting Party will not experience any adverse consequences in any sense whatsoever if the report was made in good faith.

Appendix I – Incidents Judgement

1. Examples of (possible) incidents

1. In the letter of 23 December 2022, the AFM gave a number of examples of (possible) Incidents divided in the subjects (i) information Security Incidents, and (ii) integrity Incidents.

(i) Information Security incidents:

1. Theft or loss of ICT resources with confidential data of Altera.
2. Unauthorized access to Altera's ICT infrastructure, possibly with result in unauthorized transactions.
3. The installation of malware on Altera systems.
4. A Data Breach, whereby confidential information has ended up in the public domain.
5. DDoS attacks or the threat thereof.

(ii) Integrity incidents:

1. An employee, policymaker or Contractor who is suspected of and/or prosecuted for a criminal offence (economic) fact.
2. A member of the Management Board or member of the supervisory board who has (in the past) been imposed an offense fine for deliberately 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 fine by the regulatory authority (AFM) or another (foreign) regulatory authority than the AFM.
5. If a Client or a contractor of Altera has become involved in serious (economic) illegal acts.

2. Incident prioritisation

1. To make it easier to take the appropriate measures for the Incident, it is important to prioritize Incidents. The Incident prioritization 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 resolution of the Incident is required.
• Impact is the measure of the magnitude of the Incident and of the potential damage resulting from it Incident before it can be resolved.

Altera strives to comply with the below principles of 2.2 - 2.5. if the Incident is caused by Altera. Service Level Agreements regarding Incident follow up will be leading if Incidents has not been caused by Altera.

2. Incident urgency

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 labor-intensive. • The Incident leads to a significant risk of serious adverse consequences serious adverse consequences for the protection of personal data.
Medium (M)	• The damage caused by the Incident increases significantly over time. • Work is lost, but can be recovered relatively quickly.
Low (L)	• The damage caused by the Incident only Increases slightly over time. • The work that remains is not time-intensive.

3. Incident impact

Category urgency	Description

High (H)	• A relatively large number of staff were affected by the Incident and/or are unable to carry out their work don't do anymore. Several departments have been affected.
	• More than 25% of the Clients are affected and/or suffer damage in any way whatsoever as a result of the Incident. Their personal data has been compromised.
	• The financial impact of the Incident for Altera is higher than €100,000.
	• The Incident leads to a significant risk of serious adverse consequences however, has serious adverse consequences for the protection of personal data. When assessing the impact of the Data Breach, are important:
	  ○ the nature and extent of the Data Breach
	  ○ the nature of the leaked personal data
	  ○ the extent to which technical protective measures have been taken
	  ○ the consequences for the privacy of the affected persons.
	• There is reputational damage, the newspaper is made.
	• There are physical injuries.

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

4. Incident Prioritization Classes

The Incident Priority is obtained by comparing urgency and impact. Resulting from this the Incident Priorities Matrix is created.

		Impact		
		High	Medium	Low
Urgency	High	1	2	3
	Medium	2	3	4
	Low	3	4	5

5. Incident Priorities Matrix

Below the classes are elaborated with a code and colours. Reaction time is the time to react on the Incident after noticing. Addressing time is the time to inform those involved in the Incident.

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

ANNEX II
INCIDENT NOTIFICATION FORM

Name and role of person completing this form:
Signature of person completing this form:
Date:

Incident

Date and time of incident:
Name/s of person/s involved in the incident:
Characteristics of incident:
Witnesses (include contact details):

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]

_____

Appendix III – Data Breaches procedure

1. Considerations

- Altera attaches importance to the proper security of its (electronic) systems in which personal data are stored and processed.
- Nevertheless, it can never be completely prevented that a Data Breach will occur.
- Altera is obliged under the General Data Protection Regulation (GDPR) to report Data Breaches to the Dutch Data Protection Authority and to the person involved if the Data Breach if the privacy of those involved is threatened.
- 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

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 Breaches to:

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

This Procedure describes the actions to 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 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).

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

3. Definitions

Besides the definitions from the Incidents Regulations, the following definitions will apply in the Data Breach 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 Breach[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 Breaches.

[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!

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, 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.

4. Identification of Data Breach

Anyone who suspects[5] or observes a Data Breach must inform the Contact Point at Altera without any unnecessary delay, or otherwise but in any event by filling in the Data Breach form of Appendix IV – Data Breach Form 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.

5. Assessment of Data Breach

Based on the information obtained, and if a Data Breach is suspected, the Management Board and the Data Protection Officer will jointly assess as soon as possible whether a Data Breach has actually occurred. The internal compliance officer may furnish advice in this regard.

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 those involved.

If the Incident has not resulted in the loss or unlawful Processing of Personal Data, a Data Breach 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 breach to 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. Cooperation with data provision regarding the Data Breach

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

- What happened? (description of the incident)
- Did it happen by accident or was it caused by malicious intent (think hacked data)?
- When did it happen? (date and time)
- When was it discovered?
- What kind of data (registers) have been leaked?
- Is the data encrypted, and if so how?
- Could the data be erased or made inaccessible remotely, and if so, did that happen?
- What are the possible consequences for those involved?
- Which group(s) of people are/have been affected?
- How many people are (approximately) affected 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. Staff availability after Data Breach discovery

The person responsible of 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, is able to take organizational measures to limit the consequences of the Data Breach, keep themselves available for consultation with the Contact Point or possibly experts appointed by him for the work assigned to him if necessary as a result of the Data Breach.

8. 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 Breach 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 Breach.

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].

9. Consequences of reporting Data Breaches

2. If the Data Breach has negative consequences for those involved, the **contact point** will do everything possible to limit these consequences as much as possible.
3. Depending on the nature and extent of the Data Breach for those involved, the **contact point** determines:
    - how those involved are informed (including in any case the announcements are made about which types of personal data have been affected, what the possible consequences are, what measures Altera takes and how those involved can prevent or (limit) the damage themselves
    - which aftercare those involved receive
    - which actions are necessary in the interest of the organization.
4. If a Data Breach has occurred – regardless of whether it has been reported or not – adequate technical and/or **organizational** measures will be taken as soon as possible to prevent future similar Data Breaches.

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

10. Assessment as to whether Data Breach should be reported to those involved (Article 34 GDPR)

Together with the Data Protection Officer, the Management Board will determine whether the Data Breach must be reported as well to the persons whose data it concerns.

An external lawyer may furnish advice in this regard.

11. Causes and corrective measures at the Contractor

The Contractor at which the Data Breach arose must, in observing the Data Breach, take, at its own expense and risk and in consultation with Altera, any necessary measures to stop the Data Breach 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 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. 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 Data Breaches, so similar situations can be avoided. Every Data Breach will be recorded in the Data Breaches Register within the system Privacy Perfect and will possess of the below points:

- A description of the incident;
- date and time of the Data Breach;
- date and time discovery of the Data Breach;
- description of the type of personal Data Breach;
- description of the category(s) of persons affected;
- approximate number of persons involved;
- whether data of individuals in other EU countries have also been leaked;
- whether the incident has been reported to the Dutch Data Protection Authority and if so, date and time of notification;
- whether the incident has been reported to the those involved and, if so, the date and time of the report;
- how those involved have been informed;
- the consequences of the Data Breach, stating the date and time if possible; and
- which technical and/or organizational measures have been taken after the Data Breach, stating the date and time.

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

13. Review

This Policy is reviewed annually.

Appendix IV – Data Breaches Form

At	Data Processing Officer (FS) / Privacy Officer (FS)
From	
Extension number	.....
Date	-- month year

About Data breach form: attn. directly a data breach at the DPO (FS) (verbally/by e-mail). This form serves to assess whether a data breach must be reported to the DPA within 72.

1) **Date of the data breach**

2) **Data breach description (how, what and to whom)**

3) **Did it happen by accident or was it caused by malicious intent (think hacked data)?**

4) **Which personal data has been leaked?**

5) **What damage can arise as a result/ what adverse consequences are experienced by those involved/ whose data has been leaked because of this?**

6) **Can the data be erased remotely or made inaccessible, and if so, has that been done?**

7) **How many persons (whose personal data is involved) are involved in the data breach?**

8) **Has 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 e-mail, promise of the deletion of the mail by the recipient who received it unintentionally, etc. and please add documents to this form if possible)***

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 you for filling in!

Assessment/motivation whether a data breach should be reported to the DPA or to those involved (to be completed by DPO/PO):