Securitas Integrity Reporting Policy

Handling investigations of complaints regarding possible violations of Securitas' policies (including Securitas' Values and Ethics)

Preliminary Remarks: This Policy is valid for all companies worldwide of Securitas AB, Stockholm, Sweden (hereafter «Securitas» – of which the Swiss company carrying the same name is not an affiliate), represented in Switzerland by Protectas SA, its branch offices and affiliates.
The terms used hereafter to name individuals or functions are valid for all employees, partners or stakeholders. Likewise and for the sake of easy reading, the male gender also represents the female gender and vice versa.

1 Introduction

Securitas' Values and Ethics Code (the «**Code**») sets out certain guiding business ethics principles that Securitas expects all of its employees to adhere to at all times.
The purpose of this integrity reporting policy (the «**Policy**») is to set out the main framework for reporting and managing any complaints raised by employees or third parties against a Securitas employee or director for a breach of the Code.
The Policy is subject to applicable law. Where the terms of this Policy, in comparison to applicable law, provides for stronger or additional safeguards, rights or remedies to employees, the terms of this Policy will apply. Due to the significantly differing rules and regulations on data processing and integrity (as well as other relevant areas) in the Securitas countries, Securitas subsidiaries may adopt complementary local policies that set out necessary deviations from the policy due to local regulations. Such policies should be approved by the Group CSR Officer.

Securitas AB holds the overall responsibility for the Securitas Values and Ethics and the data processing within the Securitas Integrity Line, but the ultimate responsibility rests with each individual country that allows processing of data for its employees in the system. Between Securitas AB and the local legal entities as well as with the External Supplier (as defined below), Data Processing Agreements are signed that regulate the relationship between the parties in the processing.
The Policy applies to all entities within the Securitas Group that have implemented the Securitas Integrity Line as of the date of that implementation. For the time being, it does not apply to the North American region, which is currently on a separate system.

2 Scope

Securitas encourages and expects all employees to report incidents on non-compliance pertaining to potential violations of laws, regulations or company policy (including the Code).
Such reporting of violations can be done in many ways, the most common of which is reporting done to a local manager, HR representative or legal/risk manager. In order to facilitate reporting in more sensitive situations, Securitas has also established the Securitas Integrity Line, which is a web-based compliance management system, operated by a third party supplier. The Securitas Integrity Line system will be managed by Securitas, following the rules of this Policy, to ensure the integrity of the system and safeguard the information reported.

Due to local data protection legislation (among other things), not all matters may be reported through the type of data processing that the Securitas Integrity Line entails. In order to safeguard the processing of reports that cannot be managed through the Securitas Integrity Line, Securitas also operates a paper-based system for filing and processing complaints as described herein. This system follows the same principles as the electronic version of the Securitas Integrity Line other than the electronic processing and systematizing of data and seeks to achieve the same level of integrity and accountability.

For certain countries, reporting of individuals using the Securitas Integrity Line must be limited to alleged or suspected incidents involving management or key employees of Securitas. For the countries in which such restrictions apply, this means for Securitas managers holding a minimum position as branch manager (or the local equivalent thereof) and above. For the relevant countries where these restrictions apply, incidents concerning individuals holding other, less senior level positions within Securitas should not be reported via the Securitas Integrity Line. Instead, regular internal reporting channels or a paper based reporting should be used.
Securitas assures that there will be no retaliation or other negative consequences for persons reporting incidents in good faith.
Securitas encourages all forms of reporting of non-compliance with its policies. In such countries where the law so requires, the Securitas Integrity Line may only be used as an ultimate remedy, that is, if no other means are available to solve the matter. In other countries with different regulations and traditions, it is the preferred method of reporting. Making reports through the Securitas Integrity Line is always voluntary and serves as a complement to the normal reporting structure.

3 Procedure for electronically processed reporting

3.1 Reporting within the Securitas Integrity Line

A complaint may be submitted openly or anonymously to Securitas' appointed third party reporting vendor (the «**External Supplier**») as follows:

(i) By telephone using the Securitas Integrity Line numbers detailed on the site.
(ii) Via the internet at securitasintegrity.com.

3.2 Information to and status of the reporting person

When a reporting person uses the Securitas Integrity Line, certain information may be provided to the person reporting. Local variations to these messages may apply for an individual country, in which case such deviations should be notified to the Group CSR Officer before implementation.

If the reporting person indicates that he or she wants to remain anonymous, the External Supplier or the Securitas Integrity Line messages will inform him or her that anonymous reporting may have the consequence that it may be difficult to conduct a detailed investigation into the complaint or alleged violation. For some countries, anonymity will not be allowed due to local regulations.

If the reporting person insists on remaining anonymous vis-à-vis Securitas, and this is not prohibited by local law, the identity of the reporting person may only be revealed by the External Supplier to Securitas or a third party, if:

(a) it is necessary for the investigation of the complaint or alleged violation or subsequent legal proceedings and the reporting person has agreed in advance to reveal his identity, or

(b) it is required by law or an important public interest.

Securitas Integrity Line will provide the reporting person means to enable the reporting person to check the status of the complaint or violation reported by him or her and leave additional information or answer questions (voluntarily) posed by the investigators (if applicable).
If reports are received via telephone, the External Supplier will draw up a written record and lodge a report on the Securitas Integrity Line. The report will mention the date that the employee reported the complaint or alleged violation of the Code.
Unless local laws and regulations allow otherwise, the report should only contain information that is strictly and objectively necessary to verify the complaint or alleged violation and will express that the facts are alleged.
The reporting person will have access to the report via a log-in code and shall be allowed to complement and request changes to the report by using said log-in code.

If the reporting person has requested to remain anonymous, the report will not contain the name of the reporting person.
As soon as practicably possible, and at the latest within 5 business days after receipt of the report, Securitas will initiate an investigation of the complaint or alleged violation. The complaints will be assigned to a designated investigator (the «**Designated Investigator**») according to the escalation process set out in Exhibit 1.
The Group CSR Officer is responsible for that the system of investigations is properly managed, but the investigations will be performed at different levels in the Group by Designated Investigators. If the report concerns the CSR Officer himself or herself or his or her immediate manager, the report shall be managed by the Group General Counsel, who will then be responsible for the coordination and management of the investigation.

3.3 Information to the reported person

The Designated Investigator will inform the reported person as soon as practicably possible after receipt of the report, unless there is substantial risk that notification of the reported person would jeopardize the ability of Securitas to effectively investigate the complaint or alleged violation or gather the necessary evidence. The reported person will then be informed as to: the facts he or she is accused of, who will receive the report, the fact that Securitas is responsible for the processing of personal data in the context of this Policy, as well as how to exercise his or her right of access and correction, but excluding the identity of the reporting person.
In the event the reported person cannot be informed immediately because of the risk set out above, Securitas will inform him or her as soon as such risk ceases to exist and in any event no later than required by applicable law.
The Designated Investigator dealing with the report will in any event assess the possibility as well as advisability

to inform the reported person. This evaluation will take into account other measures that can take away the objections against informing the reported person immediately, including, but not limited to, technical and organisational measures that can be taken to prevent the destruction of evidence.

After the reported person has been informed of a report, he or she will be interviewed to enable the reported person to give his or her view on the facts on which the report is based. The reported person who has been informed of a report will also be notified as soon as possible whether or not he or she will be suspended (if permissible under applicable law and deemed appropriate) during the further investigation of the claim or alleged violation. After the investigation has been concluded, Securitas will seek determine within two (2) months what actions will be taken. Once such decision is made, the reported person will be informed if and what action will be taken as a consequence of the report. If the reported person is informed that no action will be taken, any suspension of the reported person (if applicable) will from that date automatically terminate.

4 Procedure for non-electronic and systematic processed reporting

4.1 Reporting outside the Securitas Integrity Line

A complaint outside the Integrity line and the normal reporting channels may be submitted openly or anonymously to Securitas as follows:

- By telephone, e-mail, regular mail or in person to a local manager, HR representative or legal/risk manager
- By telephone, e-mail, regular mail or in person to a divisional or regional manager, divisional HR representative or divisional or regional legal/risk manager
- By e-mail using the following address: integrity@securitas.com
- By regular mail to: Group CSR Officer, P.O. Box 12307, S-102 28 Stockholm, Sweden

4.2 Information to the reporting person

If the reporting person indicates that he or she wants to remain anonymous, Securitas will inform him or her that anonymous reporting may have the consequence that the complaint or alleged violation may be difficult to investigate. For some countries, anonymity will not be allowed due to local regulations.
Securitas will draw up a written record. The report will mention the date that the reporter reported the complaint or alleged violation of the Code. Unless local laws and regulations allow otherwise, the report will only contain information that is strictly and objectively necessary to verify the complaint or alleged violation and will express that the facts are alleged. The reporting person shall be allowed to make additions to and request changes to the report.

If the reporting person has requested to remain anonymous, the report will not contain the name of the reporting person.
As soon as practicably possible and at the latest within 5 business days after receipt of the report, Securitas will initiate an investigation of the complaint or alleged violation. The complaints will be assigned to a designated investigator (the «**Designated Investigator**») according to the escalation process set out in Exhibit 1.

The Group CSR Officer is responsible for that the system of investigations is properly managed, but the investigations will be performed at different levels in the Group by Designated Investigators. If the report concerns the CSR Officer himself or herself or his or her immediate manager, the report shall be managed by the Group General Counsel, who will then be responsible for the coordination and management of the investigation.

Securitas will provide the reporting person means to enable the reporting person to check the status of the complaint or violation reported by him or her and leave additional information or answer questions (voluntarily) posed by the investigators (if applicable).

4.3 Information to the reported person

The Designated Investigator will inform the reported person as soon as practicably possible after receipt of the report, unless there is substantial risk that notification of the reported person would jeopardize the ability of Securitas to effectively investigate the complaint or alleged violation or gather the necessary evidence. The reported person will then be informed as to: the facts he or she is accused of, who will receive the report, the fact that Securitas is responsible for the processing of personal data in the context of this Policy, as well as how to exercise his or her right of access and rectification, but excluding the identity of the reporting person.
In the event the reported person cannot be informed immediately because of the risk set out above, Securitas will inform him or her as soon as such risk ceases to exist and in any event no later than required by applicable law.
The Designated Investigator dealing with the report will in any event assess the possibility to inform the reported person. This evaluation will take into account other measures that can take away the objections against informing the reported person immediately, including, but not limited to, technical and organisational measures that can be taken to prevent the destruction of evidence.

After the reported person has been informed of a report he or she will be interviewed to enable the reported person to give his or her view on the facts on which the report is based. The reported person who has been informed of a report will also be notified as soon as possible whether or not he or she will be suspended (if possible and appropriate under applicable law) during the further investigation of the claim or alleged violation.
After the investigation has been concluded and under normal circumstances, Securitas will seek determine within two (2) months what actions will be taken. Once such decision is made, the reported person will be informed if and what action will be taken as a consequence of the report. If the reported person is informed that no action will be taken, any suspension of the reported person will from that date automatically terminate.

5 Protection of Personal Data

5.1 Data Controller for the Securitas Integrity Line

Securitas AB is the data controller within the meaning of the applicable data protection legislation for the processing of personal data under this Policy. Additional Group companies may be data controllers concerning personal data relating to their employees processed within the Securitas Integrity Line. Where required under applicable law, the processing of personal data has been notified to or authorised by the competent data protection authorities.

Securitas will only process personal data under this Policy for the purpose of reporting complaints and/or alleged violations of laws, regulations or company policy (including but not limited to the Code).

Unless local laws allow for wide processing, the processed personal data shall be limited to the identity, functions and contact details of the reporting person, the reported person and all persons participating in the investigation and handling of the report, the reported facts, the information gathered during the investigation, the results of the investigation and the actions that will be taken following the investigation.

5.2 Data Processor for the Securitas Integrity Line

The External Supplier acts on behalf of Securitas as a data processor within the meaning of the data protection laws. For this purpose, Securitas AB has, for itself and on behalf of the group companies, entered into a processing agreement with the External Supplier. Under this agreement, the External Supplier will:

(a) only process the relevant personal data in accordance with the instructions of Securitas,

(b) maintain strict confidentiality of the personal data and provide it only through the communication channels specified in writing by Securitas,

(c) take appropriate technical and organisational security measures to protect the personal data, including but not limited to access control to databases, reinforced confidentiality agreements with staff of the External Supplier and password protection of files,

(d) give Securitas the right to review the measures taken by the External Supplier and submit its data processing facilities to audits conducted by Securitas in connection therewith, and

(e) comply with Securitas' instructions for removal or destruction of personal data and shall in any event return all paper and electronic materials including personal data when the agreement with Securitas is terminated, unless Securitas instructs the External Supplier to destroy them, in which case, the External Supplier shall confirm in writing the performance of the destruction.

Securitas AB may also sign agreements with its subsidiaries concerning the proper processing of personal data within the Securitas Integrity Line.

The External Supplier is located in the United States and the data is processed on servers located in Canada up until December 2012 and from then in the United Kingdom. The External Supplier adheres to the Safe Harbour Principles issued by the U.S. Department of Commerce on 21 July 2000. European Commission Decision 2000/520/EC sets forth that the Safe Harbour Principles provide for an adequate level of data protection under article 25(2) of Directive 95/46/EC. The External Supplier's adherence to the Safe Harbour Principles therefore provides a valid legal basis for all transfers of personal data from Securitas to the External Supplier under this Policy.

5.3 Security

Securitas will take the necessary technical and organisational measures to adequately safeguard the personal data against loss or unauthorized access. Securitas has instructed the External Supplier to do the same. Such measures will include authentication processes and other means necessary to protect the reporting person's identity, passwords and personal identifiers, logging access to data and regular review of log files. All persons participating in the investigation and handling of the report will be bound by specific reinforced security and confidentiality obligations. The personal data may be collected by any data processing means, whether electronic or not. These means shall in all events be solely dedicated to the Securitas Integrity Line as set up under this Policy, i.e. the personal data will in all cases be processed separately from other employee information systems or employee files.

5.4 Storage and removal

Personal data relating to reports that have been found unsubstantiated or reported in bad faith will be removed. Where removal is required by law or regulation, personal data relating to reports and complaints will be removed within two (2) months after the verification work is completed, unless disciplinary action is taken or court proceedings are filed against the reported person or if the reporting person filed a report in bad faith, in which events the data will be removed within two (2) months after the disciplinary action or any court proceedings, including any appeal, have been completed.

«Remove» means destruction of the personal data or adaptation of the personal data in such a way that identification of the reported person and the reporting person are no longer possible. Securitas Group companies may implement their own principles for information retention in order to ensure that the procedure complies with local rules and regulations. After the aforementioned storage periods are lapsed, the personal data may only be kept for archiving and statistical purposes in accordance with applicable data protection legislation. Any access to the personal data will then be restricted to Group administrators of the system for specifically determined purposes only.

5.5 Transparency

Without prejudice to the other information requirements under this Policy:

(a) where appropriate or required by law, this Policy shall be translated in one or more of the local official languages. The relevant country shall be responsible for such translations, if needed,

(b) this Policy will be made available on the Integrity Line website, My Securitas or by other means which allow employees to easily access its content, and

(c) employees will be informed as to:

- (i) the existence, purposes and functioning of this Policy,
- (ii) the identity of the responsible Securitas company,
- (iii) the recipients of reports,
- (iv) the rights of a reported person to access, correction and removal of personal data relating to him or her,
- (v) any export of their personal data, insofar as required under applicable law,
- (vi) the right of a person to object to the processing of personal data relating to him,
- (vii) the fact that the identity of the reporting person will remain confidential, except if disclosing the identity is indispensable for the investigation of the complaint or alleged violation or subsequent legal proceedings, if such is required by applicable law or an important public interest or if the report has been submitted in bad faith,
- (viii) the fact that abuse of the reporting routines set up by this Policy may be sanctioned, and
- (ix) the fact that reporting in good faith shall not be sanctioned.

5.6 Rights of access/correction/removal

Any employee may, at all times, request from the Group CSR Officer confirmation of whether or not a complaint or violation has been reported about him or her. If so, he or she will be provided with a complete written overview of the personal data available about him unless this would:

(a) seriously hinder the investigation, in which case a complete written overview will be provided, once the evidence has been protected, or

(b) compromise the interests of the reporting person or the rights and freedoms of others, in which case the written overview will only include personal data that does not compromise such interests or rights.

If personal data provided under the first paragraph proves to be incorrect or irrelevant, the reported person can request correction or removal of such information. The reported person also has a right to object to the processing of personal data in relation to a report on compelling legitimate grounds relating to his or her particular situation, unless the legitimacy of the processing is based on a legal obligation.

Requests mentioned under this section will be answered as soon as reasonably practicable. In any event, a request mentioned in the first paragraph above will be answered within four (4) weeks following receipt and a request mentioned in the second paragraph will be answered within ten (10) days following receipt. Any refusal will be in writing and shall mention the reasons therefor.

5.7 Disclosure to third parties outside EEA

If it is necessary to disclose personal data to a person or legal entity in a country outside the EEA that does not ensure an adequate level of protection in the meaning of the EU data protection directive, the requirements under applicable law relating to international transfers of personal data shall be complied with.

6 Adoption of and changes to the Policy

This Policy has been adopted by Securitas AB in order to prevent, detect and correct complaints and violations of laws, regulations and company policy (including the Code) and have been implemented by Securitas.

Securitas may change this Policy from time to time without prior notice.

RE-3290-IRP-E-CH 11/2014