Group Whistleblowing Policy

1 Summary

Securitas aims to always conduct its business activities in accordance with the highest ethical standards, *20. Securitas' Values and Ethics Code* (the "Code") as well as other Group Policies set out certain values and principles that Securitas requires all its employees and business partners to always adhere to in their work for Securitas.

Securitas promotes a corporate culture where employees openly report issues of concern in the workplace to management. However, employees sometimes do not want to report, or are uncomfortable openly reporting, issues of concern to management, for example due to fears of retaliation. Knowledge about concerns is crucial to ensure that Securitas can resolve potential problems without delay.

The purpose of this whistleblowing policy (the "**Policy**") and its mandatory instructions is to set out the main framework for managing reports or complaints of misconduct raised by employees or third parties against a Securitas employee, director or officer without fears of retaliation. Misconduct can include violations of laws or regulations or non-compliance with a Securitas' policy, instruction, or the Values & Ethics Code.

Summary of main changes since last revision:

No changes.

2 Main Text of the Policy

Securitas encourages all employees, business partners or other third parties to report any suspected or known misconduct. Concerns must be raised in good faith and may be reported confidentially/anonymously. Reports of misconduct should describe in as much detail as possible the alleged unethical behavior, the individuals involved, and the basis and evidence for the allegation. When possible, supporting documentary evidence should be provided.

This policy covers the raising of concerns related to breaches of Securitas's Values & Ethics Code, corporate policies as well as laws and regulations.

Reporting of violations can be done in many ways, the most common of which is reporting done to a local manager, HR representative, Business Ethics Compliance Officer, General Counsel or Head of Legal/Risk Manager.

In order to facilitate reporting in more sensitive situations, Securitas has also established the "Securitas Integrity Line" (available at securitas.integrityline.com), which is a web-based compliance management system that allows **anonymous reporting**, operated by a third-party provider. The Securitas Integrity Line is managed by Securitas AB, 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. This system follows the same principles as the electronic version of the Securitas Integrity Line and seeks to achieve the same level of integrity and accountability.

A fundamental element of this policy is that Securitas does not tolerate any retaliation against individuals who have reported concerns in good faith. This whistleblowing service is safe, confidential, impartial, and available all hours; whistleblowers can report anonymously although that may make it more difficult to investigate the concern.

All reported matters will be investigated in a thorough, objective, and timely manner and according to the mandatory instructions related to this Policy. Reported matters are handled without influence from individuals who are or could be affected by the complaint.

The Group CEO shall issue further directives or procedures regarding whistleblowing. The task to issue further instructions or procedures can be delegated.

3 Applicability

The Policy applies to all employees and entities within the Securitas Group.

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 prevail. 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 must be approved by the Chief Business Ethics Compliance Officer.

4 Implementation and Responsibility

It is the responsibility of all Divisional Presidents, Divisional General Counsel and, through them, each Country President (or equivalent) and, local Head of Legal/General Counsel and BE responsible person, to ensure that this Policy (and the relevant local law) is fully understood and implemented in their areas or countries of responsibility.

Securitas AB holds the overall responsibility for 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 rights and obligations between the parties.

5 Training

Training on how to raise concerns is included in the Values & Ethics e-learning course which is mandatory for all employees.

6 Investigations and Consequences of Breach

Securitas encourages and expects all employees and business partners to report incidents on non-compliance pertaining to potential violations of laws, regulations or company policy (including the Code) using the channels identified in this Policy, whether they relate to Securitas, its employees, or its business partners.

Securitas has zero tolerance for ethical misconduct, and staff whose conduct breaches the requirements of the Policy may face legal and disciplinary action, including termination of employment.

7 Review and Follow-up

Compliance with this policy by all Securitas entities and employees will be monitored as part of the Business Ethics Compliance Program.

8 Reference to Instructions

The CEO has issued the following instructions related to integrity reporting:

- 26.1. Instructions to the Whistleblowing Policy

INSTRUCTION TITLE AND NO:
26.1. Instructions to Securitas Whistleblowing Policy
OWNER: Chief Ethics & Sustainability Officer
APPROVED BY: Group CEO
APPROVED DATE: 240508
TARGET AUDIENCE: Employees involved in handling reports or complaints of misconduct and/or non-compliance with Securitas policies

Instruction to Securitas Whistleblowing Policy

1 Introduction and objective

The purpose of these mandatory instructions is to set out a standard process for how reports of misconduct raised by employees or third parties against a Securitas employee, director or officer will be handled.

Summary of main changes since last revision:

— Minor changes to the description of the investigation process.
— Clarification of group responsible persons.
— Specific mention that countries need to establish their own processes, in line with this instruction.

2 How to report

Reports or complaints of misconduct can made through Securitas' confidential whistleblower system, Integrity Line, through the normal reporting channels, such as Manager, HR representative, Business Ethics Compliance Officer, Divisional General Counsel or Head of Legal/General Counsel, Risk Manager, or by sending an email to integrity@securitas.com.

2.1 Reporting within the Securitas Integrity Line

Securitas Integrity Line, is managed by a third party vendor (the "**External Supplier**")

A report about misconduct may be submitted to the Securitas Integrity Line, either:

(i) Via the internet at securitas.integrityline.com (outside the US, Canada and Mexico)
(ii) Via www.securitashotline.com for the US, www.securitashotline.ca for Canada and www.lineadealerta.com.mx for Mexico
(iii) By telephone using the numbers detailed on the respective site (only for US, Canada and Mexico).

If the reporting person indicates that they want to remain anonymous, the Integrity Line will inform them that anonymous reporting may make it more difficult to conduct a detailed investigation into the complaint or alleged violation. Securitas encourages whistleblowers to provide their contact details when raising ethical concerns so that additional information may be easier to obtain.

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

a) The reporting person has agreed in advance to reveal their identity, or
b) it is required by law or an important public interest.

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

If reports are received via telephone, the External Supplier will write a 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.

The reporting person will have access to the report via a log-in code as long as the report remains open and shall be allowed to complement and request changes to the report by using this log-in code. If the reporting person has requested to remain anonymous, the report will not contain the name of the reporting person.

2.2 Reporting outside the Securitas Integrity Line

A complaint outside the Securitas Integrity Line and the normal reporting channels may be submitted openly or anonymously to Securitas as follows (but not limited to):

- By telephone, e-mail, regular mail or in person to a local manager, HR representative, Business Ethics Compliance Officer, Divisional General Counsel or Head of legal/Risk Manager.
- By telephone, e-mail, regular mail or in person to a Divisional or Regional Manager, Divisional HR representative, Business Ethics Compliance Officer or Divisional or Regional Legal/Risk Manager.
- By e-mail using the following address: integrity@securitas.com.
- By regular mail to: Chief Business Ethics Compliance Officer, P.O. Box 12307, S-102 28 Stockholm, Sweden.

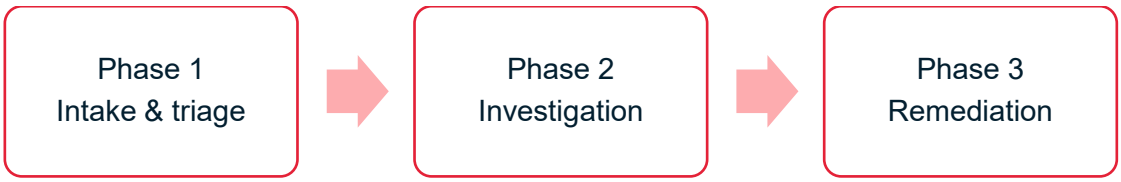
2.2.1 Notification to Group

All reports of misconduct made outside of Securitas Integrity Line must be notified to the Business Ethics function at Group and follow the standard investigation process described below under Section 3. The Group Business Ethics Team must be notified of all high or medium risk cases as soon as possible, and the case must be registered in the global Securitas Integrity line. Low risk cases can be notified on a quarterly basis or as requested by the Group Business Ethics team.

A case can be categorized as high or medium risk if it concerns a breach of law, Securitas Values & Ethics Code or corporate policies, or if it in some other way is considered to be a serious issue. A case can be categorized as low risk if it, for example, mainly concerns a personal work-related grievance. Contact the BECO for the Division if you have doubts about how to categorize a specific case.

3 Investigations

All reports of misconduct will go through the same three-stage process depicted below:



3.1 Intake & triage phase

All reports or complaints of misconduct in the Securitas Integrity Line and sent to integrity@securitas.com will initially go to the Chief Business Ethics Compliance Officer (CBEO)[1], and Divisional Business Ethics Compliance Officers (BECOs). The CBEO, together with the BECOs, will review the report and will schedule a triage assessment to prioritize investigations of reports that indicate serious material risks. The Intake and Triage phase will follow section 3.4. timing requirements.

As a result of the triage, relevant independent individual(s) (usually the General Counsel(s), and/or the Head of HR) may be included to confirm and agree on the initial assessment when needed.

If the report concerns individuals in Divisional management, the Group General Counsel must be involved, and the triage assessment may be completed without input from the Division.

The triage assessment will result in a decision to either:

a. Request more information,
b. Investigate the case, or
c. Dismiss the case

Request for more information – If during the triage phase, the CBEO or BECOs consider more information is required to decide on how to proceed, they will contact the reporter. The reporter will then have 2 weeks to provide further information.

Investigate the case - If a decision is made to investigate, the report or complaint will be assigned to a Case Manager. The Case Manager will be determined by the Risk level assessment performed during the triage phase. If the case is considered high risk, then the Case Manager will be the CBEO or respective Divisional BECO. For medium risk cases, the Case Manager will be the Divisional People, Legal, ICFR or BECO (see 3.1.1), or local responsible with Divisional oversight. Finally, in general low risk cases will be handled directly by local People, Legal or BE Responsible.

The Case Manager can be an independent internal employee of Securitas or an external investigator. The decision by Group to assign the case will be the Case Manager's authorization to conduct the investigation.

The Case Manager will plan, conduct, and report on the investigation. The respective Divisional People, (e.g. Legal, ICFR, HR or BECO) may be consulted when needed and may act as a second pair of eyes (four-eyes principle) and can give advice on the investigation plan and the report, checking against legal risk and other issues.

Dismiss the case – If the report doesn't provide sufficient or adequate information, after the 2 week period the case will be dismissed. The reporter will be informed in case they want to provide further information at a later stage.

[1] Individual intake and investigation protocols can be agreed between the Business Ethics function and a Division and a Country/Business Unit.

3.1.1 Group responsible persons

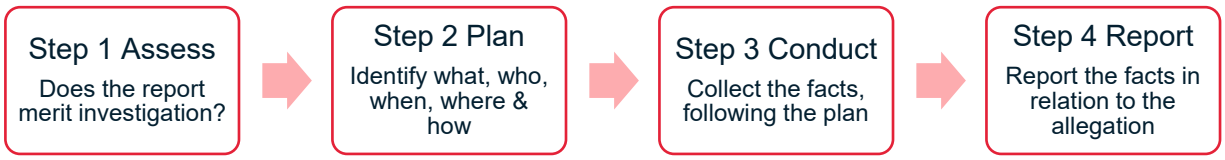
For medium and high risk cases, the respective Divisional or Group responsible managers (ICFR, People, Legal) will be involved during the triage stage and will keep oversight of the investigation to address any possible concerns.

The respective Divisional functions (e.g. HR, BE and Legal) are responsible for analyzing and following up cases in the Securitas Integrity Line on an aggregated level. The aim of the follow up is to ensure that cases are managed in a timely and proper manner and that trends are appropriately addressed. Divisional functions will also provide oversight and assistance to countries in the handling of cases.

All reported matters will be investigated in a thorough, objective, and timely manner. Reported matters are handled without influence from individuals who are or could be affected by the complaint.

3.2 Investigation phase

An Investigation will be managed by the Case Manager who will follow a standard investigation process with four separate steps. The details of each step will be described in detail in a separate Case Manager Handbook[2]. The investigation steps are depicted here and further described below:



3.2.1 Step 1 Assess – Does the matter merit investigation?

Before the Case Manager starts to plan the investigation, they should do an initial assessment about the allegations in the report and about the assignment of the case.

Before continuing to the next step, the Case Manager must:

1. Be clear about the alleged misconduct that is to be investigated and the focus of the investigation.
2. Have sufficient detail in the allegation to have an initial line of inquiry.
3. Have conducted a preliminary verification of some elements.
4. Have gone back to the reporter for further information, if required.
5. Have no personal interests that may interfere with their objectivity in the case.

In case of a report classified as low risk and the Case Manager does not believe that the matter merits an investigation, they must consult with the respective Divisional Function and properly document the reasoning behind the decision in the Securitas Integrity Line system. In case the report is graded as high or medium risk, the case manager must obtain an approval from the Divisional BECO before closing the case.

[2] In addition, investigation and documentation templates will be made available.

When the Case Manager has confirmed 1-5 above and assessed that an investigation is required they can proceed to the next step.

3.2.2 Step 2 Plan – Identify what, who, when, where & how

An investigation is a process of answering the following question: ***"do the facts support an allegation or not?"*** The focus of an investigation is on the fact not opinions, hypotheses, or rumors.

Each investigation depends on the unique facts connected to the allegations, but as a general rule, investigators must keep an open mind, be thorough, challenge witnesses on the facts, seek the details, interview all the relevant witnesses, review all relevant documents and not accept statements without verification.

In this step the Case Manager must establish an investigation plan to identify the facts that are relevant to the alleged misconduct. The plan starts with an analysis of who did what, how, when and where and should be documented in the Securitas Integrity Line for high and medium risk cases. The investigation plan for low risk cases may be documented locally in the country.

If it is deemed necessary to conduct a search of a current or former employee's email account or review other files, for example, financial records or credit card statements, this may have to be approved separately.

The Case Manager will document the plan in the Securitas Integrity Line for high or medium risk cases. If there are any specific legal risks or requirements that may apply in the jurisdiction, the Case manager should consult with the respective Divisional Function to ensure the plan is fit for purpose. In case of reports classified as low risk the investigation plan may be documented outside of the Securitas Integrity Line, however the Case Manager is encouraged to seek advice from the Divisional Functions if needed.

3.2.3 Step 3 Conduct – Collect the facts following the plan

In this step the Case Manager executes the actions identified in the plan. The key to implementing a successful plan is to break down each of the actions into an activity, usually finding information in documents or emails or through interviews of people.

The activities carried out in the investigation should provide answers to the questions laid out in the plan, i.e. who did what, how, when and where.

When conducting an investigation it is important that the knowledge of the case is limited to as few people as possible. This is important for three reasons; the alleged misconduct is not yet substantiated and we therefore need to respect the dignity and reputation of the person who has been accused of misconduct. Secondly, we want to protect the whistleblower from potential retaliation. Finally, if there has been misconduct, it is possible that the person concerned will take steps to remove evidence or otherwise tamper with the investigation.

3.2.4 Step 4 Report – Report the facts in relation to the allegation

The purpose of the investigation is to learn the facts and draw conclusions as to whether or not an allegation of misconduct is substantiated, and when substantiated, take action to correct the behavior and/or its consequences.

Once the investigation is complete, the facts need to be assembled in a written report. The report must include records of interviews and evidence from document searches or other records. The report should also propose a finding on whether the case is substantiated or not substantiated and remediation proposals. The report will form the basis for subsequent management discussion and decision regarding any consequences that may result from the case.

In all cases received via the Securitas Integrity Line the report should be documented in the Securitas Integrity Line system. The final report, in case of high or medium risk cases, should always be reviewed by the relevant Divisional functions before the investigation phase is concluded and the next remediation phase is initiated.

If the conclusion is that the case is unsubstantiated the Case Manager must inform the reporter that the case has been investigated but that we were unable to find facts that substantiated the allegation(s) and the case can be closed.

3.3 Remediation phase

Remediation is the action taken to remedy the causes and consequences of substantiated misconduct and is the primary objective of the investigation process.

The remediation phase begins with the dissemination of the investigation report to the applicable business leader(s) on a strict and confidential need to know basis, and to the respective responsible Group person(s). The applicable business leader(s) may request that other functional staff participate, such as Head of Finance, General Counsel/Head of Legal or Head of HR.

To review the report, the appointed Case Manager convenes a remediation meeting with participation by the applicable business leaders as defined by the local process description. The responsible Divisional Function may be invited and must participate in case of high or medium risk cases.

At the meeting the report is presented and the participants assess the finding and the remediation proposals. The remediation discussion starts with the findings and remediation proposals identified in the investigation report but the meeting must also conduct a root cause analysis to understand the failures that caused the report or complaint to be filed with the purpose of preventing it from happening again.

The result of the remediation meeting should be to agree on a remediation plan which must contain details on:

- The agreed remediation actions,
- The manager(s) responsible for implementing the actions,
- Timelines for implementation of the actions, and
- Subsequent monitoring, e.g. after 6 months to continued compliance

The internal remediation actions can, for example, include disciplinary action, reassignment of personnel, re-training of personnel, revision of relevant steering documents, improvements to internal controls and processes. In addition, there may be external actions such as legal actions against third parties and the possibility of notification to applicable authorities (e.g. the police).

In all cases received via the Securitas Integrity line the remediation plan must be documented in the Securitas Integrity Line system.

3.3.1 Close the case

If the conclusion is that the case is unsubstantiated, the Case Manager must inform the reporter that the case has been investigated but that we were unable to find facts that substantiated the allegation(s), and the case can be closed.

Similarly, when the remediation plan has been agreed, the Case Manager must inform the whistleblower that the case has been investigated and that management is taking appropriate action.

The Case Manager may also notify witnesses that the case is being closed and remind witnesses of the duty of confidentiality. The records of the investigation shall be kept in the whistleblower system, Integrity Line, in case the original report came through this channel. Low risk reports received through other channels may be stored locally as defined in a local process.

3.4 Timing

Investigations must be performed in a timely manner. The following timeframes apply to all investigations:

- *Acknowledgement of receipt of the whistleblower report* should be sent to the reporting person as soon as possible and no later than seven (7) days after the report was received. The Business Ethics Team is responsible for managing this process for reports received via the Securitas Integrity Line.
- *Finalization of the investigation and feedback to the reporter* should be done within three (3) months of receiving the whistleblower report by the case manager. (as an exception, highly complex investigations may extend beyond this period but must be closely monitored by the Group or divisional responsible person).

4 Protection of personal data

Information on the protection of and processing of personal data can be found in *Exhibit 1*.

5 Applicability

These instructions are mandatory and apply to all companies, employees, directors and officers of companies within the Securitas Group, that is, companies where Securitas AB (publ) directly or indirectly, owns or has a controlling interest.

6 Implementation and responsibility

Group will be responsible for managing the Securitas Integrity Line and for providing training material and templates necessary for Case Managers to conduct investigations. Group will also develop standard information material for Securitas Integrity Line and for the Investigation process described in this instruction.

It is the responsibility of all Divisional Presidents and, through them, each Country President, to ensure that this Policy is fully understood and implemented in their areas or countries of responsibility.

Each country should have a process description, in line with this Instruction, that describes how cases managed locally are triaged, investigated, and remediated. This description should include both the management of cases coming through the Securitas Integrity Line, as well as those submitted outside the Securitas Integrity line.

The aim of the process is to ensure an independent investigation and a fair and balanced remediation for all cases managed locally, depending on applicable local law.

7 Consequences of breach

Violations of these instructions may result in disciplinary action appropriate to the violation, including, but not limited to, termination of the employment. It may also result in fines or penalties for which the individual may be held responsible.

8 Review and follow-up

Compliance with these instructions by all Securitas entities and employees will be monitored through internal and external audits, and routine follow-ups of all reported matters.

_____

Exhibit 1

Protection of personal data

For information on what Securitas company are processing your information and how to get in contact with us, please see the Personal Data Controllers document, which you can find at the end of this document in the appendix.

The Personal Data Controllers document also covers any amendments or modifications to this Privacy Notice that applies to a specific country, so called Country Unique Terms. If a part of the Privacy Notice is amended by specific Country Unique Terms the remainder of the Privacy Notice remains unchanged. Relevant changes are listed under each country, if nothing is listed, there are no local variations.

We at Securitas ("**Securitas**", "**we**" or "**us**") respect your integrity. This Privacy Notice for the Securitas Integrity Line describes how we collect and process personal data in connection with our confidential and secure reporting platform which can be used to report incidents and raise concerns about misconduct, wrongdoing, violation of laws, regulations or non-compliance with Securitas' applicable policies. To read more about our Values and Ethics Code visit the Values & Ethics code tile.

It is important for us that you read and understand this Privacy Notice before you use the Securitas Integrity Line. You are welcome to contact us if you have any questions.

Responsibility for the processing of personal data

The relevant local Securitas entity which has received the incident report together with Securitas AB are jointly responsible (joint controllers) for the processing of personal data in the Securitas Integrity Line. To ensure that your personal data is protected, we have entered into a joint arrangement regarding the use and protection of your personal data. This Privacy Notice reflects the essence of our joint arrangement. If you wish further information on the arrangement, you are welcome to contact us.

Categories of personal data

The information outlined below will be processed in connection with the use of Securitas Integrity Line and any investigation of a submitted incident report. Which categories of personal data that will be processed in the specific case depend on the contents of the incident report, the information provided by the reporting person and which information that is deemed relevant for the investigation.

Moreover, the reporting system allows a reporting person to submit reports and communicate anonymously via an encrypted connection, in which case no personal data will, as a starting point, be

collected from the reporting person, unless the reporting person voluntarily provides personal data in the incident report as such or in subsequent communication.

Personal Characteristics and Identifiers: First and last name.

Personal Directory Information: E-mail address, phone number, video footage, pictures or voice recordings

Business Contact Information: Your role, title, the business that you work for.

Incident and case information: Details regarding the reported incident, the designated Case ID.

Communication: Contents of e-mails, messages or other communication.

Audit Trail data (Technical information): IP address, version of operating system and browser.

The purpose and the lawful basis for the processing

Securitas is processing the personal data you as a *reporting person* provide to us when using the Securitas Integrity Line, communicating with the case managers, or which we collect from other sources in connection with an investigation of an incident.

The sources that we collect personal data from in connection with an incident report and an investigation of an incident include, besides the reporting person, the reported person(s), other persons (which may be employees or other engaged personnel or external persons) involved in an investigation, legal advisors, public authorities, and publicly available information sources, for example information available on the Internet or public records.

Purpose of processing	Lawful basis for processing	Retention period
We process the personal data described above to collect, manage and investigate incident reports submitted through the Securitas Integrity Line, including to review and evaluate the report, communicate with the reporting person and other persons relevant to the investigation of the incident report and document the measures taken to investigate the reported incident.	*The Securitas company responsible for investigating the report:* To the extent the Securitas company is legally obligated to collect and manage incident reports, the processing is necessary to comply with a legal obligation. Where there is no legal obligation for the Securitas company to collect and manage incidents, the Securitas company relies on its	Personal data collected in connection with an incident report will be stored for this purpose during the investigation of an incident and for a period of two (2) years following the date the case was closed.

	legitimate interest to manage incident reports and investigate alleged misconduct, wrongdoing, violation of laws, regulations or non-compliance with Securitas' applicable policies. *Securitas AB and other relevant Securitas companies:* The processing is necessary to satisfy Securitas AB's and the relevant Securitas company's legitimate interest to manage incident reports and investigate alleged misconduct, wrongdoing, violation of laws, regulations or non-compliance with Securitas' applicable policies.	
We process Incident and case information collected through Securitas Integrity Line to analyze incident reports on an aggregated level and produce statistics.	The processing is necessary to satisfy Securitas AB's and the relevant Securitas company's legitimate interest to analyze incident reports on an aggregated level and produce statistics. This helps us better understand, for example, how many incident reports that are submitted using the reporting platform and what types of incidents that are reported.	Personal data is stored for this purpose for the same period as incident reports are stored in the reporting platform, which means that the personal data will be stored for a period of two (2) years following the date the case was closed. Information on an aggregated level and statistics which do not include any personal data may be stored until further notice or until it is deleted.
We process and share relevant personal data with public authorities, Securitas group companies, legal advisors, trade unions and works councils where necessary to manage and defend legal claims as a result of an incident report. This includes reporting the incident to law enforcement where applicable.	The processing is necessary to satisfy Securitas AB's and the relevant Securitas company's legitimate interest to manage and defend legal claims.	Personal data is stored for this purpose for the period required in order for us to manage and defend the legal claim in the specific case.

We process the personal data stored in the Securitas Integrity Line to ensure technical functionality and security of the reporting system, including ensuring that personal data in the Securitas Integrity Line is only accessed by authorized case managers, in connection with logging for troubleshooting and incident management and to keep backups of personal data to ensure the availability of the personal data processed in case of a technical or physical issue.	The processing is necessary to satisfy Securitas AB's and the relevant Securitas company's legitimate interest to ensure technical functionality and security of the reporting system.	Personal data is stored for this purpose for the same periods as outlined above.

Who do we share your personal data with?

EQS Group: Your personal data will be processed by our service provider EQS Group AG ("**EQS Group**"), which provide the reporting platform used for the Securitas Integrity Line and their sub-processors (which provide for example hosting and translation services) on instruction from Securitas. EQS Group AG acts as Securitas personal data processor and is under contractual arrangements only allowed to process data for the purposes as set out above. EQS Group does not have access to incident reports in the reporting platform, unless specifically authorized by Securitas.

Other service providers: In addition, in connection with an investigation of an incident report, your personal data will be processed by other service providers or subcontractors that we have engaged, including data storage service providers and suppliers of productivity and communication tools, when the case manager uses tools provided by such service providers to carry out the investigation. All service providers and subcontractors act as Securitas personal data processors and are under contractual arrangements only allowed to process data for the purposes authorized by Securitas. Furthermore, the personal data processor (service provider or subcontractor) and those acting under instructions of the processor will not access more personal data than is required for the performance of the service covered by the agreement with Securitas.

Securitas Group: Where an incident report concerns another company within the Securitas Group, the personal data collected in connection with an incident report may be shared with the Securitas company if necessary to investigate the incident and, where necessary, to manage and defend legal claims as a result of an incident report.

Public authorities: Securitas shares your personal data with public authorities (such as the police, the tax authority, or other authorities) where necessary to manage and defend legal claims. Public authorities that receive your personal data will be the controller for such processing, which means that it is not Securitas who governs how your personal data is processed if shared with an authority. Thus, if your personal data is shared with authorities, this Privacy Notice will not cover that subsequent processing.

Legal advisors: Where necessary to manage and defend legal claims as a result of an incident report, we share personal data with legal advisors that we have engaged. Normally the legal advisor is responsible (controller) for its own processing of personal data when providing legal advice and services.

Insurance companies: Where necessary to manage and defend legal claims as a result of an incident report, we share personal data with insurance companies, for example to file an insurance claim as a result of an incident (as applicable). The insurance company is responsible (controller) for its own processing of personal data when managing an insurance claim or matter.

Trade unions and works councils: Securitas share personal data, where necessary, with trade unions and works councils to manage and defend legal claims as a result of an incident report, including to take employment law measures (warnings and termination of employment with or without notice), where appropriate, against the reported person. Trade unions and works councils are responsible (controller) for their own processing of personal data.

Where we are processing your personal data

To provide you with the Securitas Integrity Line, we and EQS Group, which processes personal data on our behalf, process your information primarily within EU/EEA. We have entered into confidentiality and data processing terms with EQS Group to ensure they comply with high levels of confidentiality, data protection laws, and best practices in privacy and security standards.

If you, however, use the Securitas Integrity Line from a country outside of the EU/EEA (a third country), your personal data will be transferred to the country that you access the Securitas Integrity Line from.

Moreover, certain services connected to the reporting platform, for example translation services, are carried out by subcontractors to EQS Group in third countries. To ensure that your data is sufficiently safeguarded outside the EU, we have ensured that there are appropriate safeguards in place, including the EU Standard Contractual Clauses (SCC), to ensure an essentially equivalent level of protection for your personal data.

How we protect your data

Securitas and EQS Group take appropriate technical and organizational measures to protect your personal data in the reporting platform and ensure that your personal data is secure in the platform. Personal data processed in the reporting platform is stored encrypted in a secure database. Moreover, communication between your web browser and the reporting platform is encrypted to ensure that your personal data is protected against unauthorized disclosure or access. Only authorized case managers will have access to incident reports in the reporting platform.

Your rights

We respect your integrity and your rights under legislation related to the processing of personal data. The rights you have means that you can request a copy of the personal data we process about you,

request incorrect information about you to be corrected, and even under certain conditions, request the erasure of information.

In certain jurisdictions your rights may be restricted, for example the right to a copy of your personal data, given that an incident report and investigations as a result of a submitted incident report is subject to confidentiality under law. This in order to protect the reporting person and other persons involved in an investigation of an incident report.

In addition, the right to data portability does not apply, since the processing of personal data is not based on an agreement with you or your consent as shown in the table above. Finally, it is Securitas' view that you normally cannot successfully object to the processing of personal data in the reporting platform given the nature and purpose of the processing.

To exercise your rights, don't hesitate to get in touch with your local Securitas entity on the contact details provided in the Personal Data Controllers document, which you can find at the end of this document in the appendix.

You also always have the right to lodge complaints to the Swedish Authority for Privacy Protection (or your national equivalent) if you have objections to our processing of your personal data.

_____