



# Weisung der Securitas AB für die Meldung von Integritätsproblemen

## Ablauf der Untersuchungen bei Beschwerden wegen möglichen Verstössen gegen Weisungen von Securitas AB (einschliesslich der Werte und ethischen Grundsätze von Securitas)

Anmerkung: Diese Weisung wurde weltweit für alle Gesellschaften der **Securitas AB** mit Sitz in Stockholm, Schweden (hiernach «Securitas» - die in keiner Weise mit der gleichnamigen Schweizer Gesellschaft verwandt ist) erstellt, welche in der Schweiz durch **Protectas SA** sowie ihre Zweigniederlassungen und Tochtergesellschaften vertreten ist.

Die hiernach verwendeten Personen- und Funktionsbezeichnungen gelten für alle Mitarbeitenden, Partner oder andere Beteiligte. Die verwendete männliche Form bezieht selbstverständlich die weibliche Form mit ein. Auf die Verwendung beider Geschlechtsformen wird lediglich mit Blick auf die bessere Lesbarkeit des Textes verzichtet.

### 1 Einleitung

Securitas erwartet, dass sich ihr gesamtes Personal jederzeit an die unternehmensethischen Leitlinien hält, die im Werte- und Ethikkodex von Securitas («**Kodex**») festgelegt sind.

In der vorliegenden Weisung für die Meldung von Integritätsproblemen («**Weisung**») wird der allgemeine Rahmen für die Meldung und Bearbeitung von Beschwerden festgelegt, die von Mitarbeitenden oder Dritten gegen einen Mitarbeiter oder Verwaltungsrat wegen Verstössen gegen den Kodex eingereicht werden.

Die Weisung gilt vorbehaltlich der anwendbaren Rechtsvorschriften. Bieten die Bedingungen dieser Weisung gegenüber den anwendbaren Rechtsvorschriften den Mitarbeitenden weitergehende oder zusätzliche Schutzmassnahmen, Rechte oder Rechtsmittel, sind diese Bedingungen massgebend. In den Ländern, in denen Securitas tätig ist, können in Bezug auf die Datenbearbeitung und die Integrität (sowie in weiteren massgebenden Bereichen) unterschiedliche Gesetze und Vorschriften bestehen; die Tochtergesellschaften von Securitas können deshalb ergänzende lokale Weisungen erlassen, in denen die erforderlichen Abweichungen von dieser Weisung aufgrund der lokalen Vorschriften festgelegt sind. Eine solche Weisung sollte dem Leiter CSR (Corporate Social Responsibility = unternehmerische Sozialverantwortung) der Gruppe zur Genehmigung vorgelegt werden.

Obwohl Securitas AB die Gesamtverantwortung für die Werte und ethischen Grundsätze von Securitas und für die Datenbearbeitung im Rahmen der Securitas Integrity Line trägt, liegt die letztliche Verantwortung bei jedem einzelnen Land, das zulässt, dass im System Daten über seine Mitarbeitenden bearbeitet werden. Zwischen Securitas AB und den lokalen juristischen Personen sowie mit dem Externen Anbieter (gemäss der nachstehenden Definition) werden Datenbearbeitungsvereinbarungen abgeschlossen, welche die Beziehung regeln, die bei der Bearbeitung zwischen den Parteien besteht.

Die Weisung gilt für alle juristischen Personen innerhalb der Securitas Gruppe, welche die Securitas Integrity Line eingeführt haben, ab dem Datum von deren Einführung. Für die Region Nordamerika, die zurzeit einem gesonderten System untersteht, gilt sie vorläufig nicht.



## 2 Geltungsbereich

Securitas fordert alle Mitarbeitenden auf und erwartet von ihnen, dass sie Vorfälle melden, die mögliche Verstösse gegen Gesetze, Verwaltungsvorschriften oder gegen die Unternehmenspolitik (einschliesslich des Kodex) betreffen.

Eine solche Meldung von Verstössen kann auf verschiedene Weise erfolgen; meistens erfolgt sie an eine Führungskraft, eine Ansprechperson in der Personal- oder Rechtsabteilung oder einen Risikomanager vor Ort. Um Meldungen in heikleren Situationen zu erleichtern, hat Securitas zudem die Securitas Integrity Line eingerichtet, ein webbasiertes System für das Compliance Management, das von einem Drittanbieter betrieben wird. Securitas betreibt das System der Securitas Integrity Line nach den Regeln dieser Weisung, um die Integrität des Systems sicherzustellen und die gemeldeten Informationen zu schützen.

Aufgrund der lokalen Datenschutzgesetzgebung (unter anderem) dürfen nicht alle Angelegenheiten über die Securitas Integrity Line gemeldet werden, da diese eine bestimmte Art der Datenbearbeitung mit sich bringt. Um die Bearbeitung von Meldungen sicherzustellen, die nicht über die Securitas Integrity Line erfolgen dürfen, betreibt Securitas auch ein papiergestütztes System für die Einreichung und Bearbeitung von Beschwerden gemäss der Beschreibung in dieser Weisung. Abgesehen von der elektronischen Bearbeitung und Systematisierung der Daten beruht dieses System auf den gleichen Grundsätzen wie die elektronische Version der Securitas Integrity Line und strebt das gleiche Integritäts- und Verantwortlichkeitsniveau an.

In einigen Ländern dürfen über die Securitas Integrity Line nur mutmassliche oder verdächtige Vorfälle gemeldet werden, an denen Mitarbeitende von Securitas in Führungs- oder Schlüsselpositionen beteiligt sind. Als solche Mitarbeitende gelten für Securitas in den Ländern, in denen entsprechende Einschränkungen bestehen, Führungskräfte, die mindestens die Position eines Bereichsleiters (oder die lokale Entsprechung davon) innehaben. In den Ländern, in denen diese Einschränkungen gelten, sollten Vorfälle mit Personen, die bei Securitas andere, niedrigere Positionen besetzen, nicht über die Securitas Integrity Line gemeldet werden. Stattdessen sollten die üblichen internen Meldekanäle oder papiergestützte Meldungen benutzt werden.

Securitas garantiert, dass Personen, die in gutem Glauben einen Vorfall melden, nicht mit Vergeltungsmassnahmen oder anderen negativen Konsequenzen rechnen müssen.

Securitas unterstützt die Meldung von Verstössen gegen ihre Weisungen in jeder Form. In den Ländern, in denen dies im Gesetz entsprechend vorgesehen ist, darf die Securitas Integrity Line nur im äussersten Fall genutzt werden, d. h. nachdem alle anderen Möglichkeiten zur Regelung eines Vorfalls ausgeschöpft wurden. In anderen Ländern mit anderen Vorschriften und Traditionen ist sie hingegen die bevorzugte Methode einen Vorfall zu melden. Die Erstattung einer Meldung über die Securitas Integrity Line erfolgt immer freiwillig und ergänzt die üblichen Meldekanäle.

## 3 Verfahren für elektronisch bearbeitete Meldungen

### 3.1 Meldung über die Securitas Integrity Line

Eine Beschwerde kann wie folgt offen oder anonym beim von Securitas beauftragten Drittanbieter des Meldesystems («**Externer Anbieter**») eingereicht werden:

- (i) per Telefon über die Telefonnummern der Securitas Integrity Line, die auf der Website angegeben sind;
- (ii) über das Internet unter [www.securitasintegrity.com](http://www.securitasintegrity.com)



### 3.2 Informationen für die meldende Person und deren Stellung

Benutzt eine Person die Securitas Integrity Line für die Meldung eines Vorfalls, können ihr gewisse Informationen abgegeben werden. In den einzelnen Ländern können für diese Botschaften lokale Varianten gelten; in diesem Fall sollten solche Abweichungen vor der Umsetzung dem Leiter CSR der Gruppe mitgeteilt werden.

Gibt die meldende Person an, dass sie anonym bleiben möchte, weist der Externe Anbieter oder die Securitas Integrity Line sie darauf hin, dass es bei einer anonymen Meldung schwierig sein kann, die Beschwerde oder den mutmasslichen Verstoss genau zu untersuchen. In einigen Ländern lassen die lokalen Vorschriften keine anonyme Meldung zu.

Besteht die meldende Person darauf, gegenüber Securitas anonym zu bleiben, und ist dies nach dem lokalen Recht zulässig, darf der Externe Anbieter ihre Identität gegenüber Securitas oder einem Dritten nur dann offenlegen, wenn:

- (a) dies für die Untersuchung der Beschwerde oder des mutmasslichen Verstosses oder ein späteres Gerichtsverfahren notwendig ist und wenn die meldende Person der Offenlegung ihrer Identität im Voraus zugestimmt hat; oder
- (b) wenn dies von Gesetzes wegen oder aufgrund eines wichtigen öffentlichen Interesses erforderlich ist.

Die Securitas Integrity Line ermöglicht der meldenden Person, den Status der Beschwerde oder des gemeldeten Verstosses zu prüfen und zusätzliche Informationen abzugeben oder (freiwillig) Fragen zu beantworten, die (gegebenenfalls) von den Untersuchern gestellt werden.

Geht die Meldung per Telefon ein, erstellt der Externe Anbieter einen schriftlichen Bericht und gibt bei der Securitas Integrity Line eine Meldung ein. In dieser Meldung wird das Datum aufgeführt, an dem der Mitarbeiter die Beschwerde eingereicht oder den mutmasslichen Verstoss gegen den Kodex gemeldet hat.

Sofern die lokalen Gesetze und Vorschriften nichts anderes zulassen, sollte die Meldung nur jene Informationen enthalten, die unbedingt und objektiv notwendig sind, um die Beschwerde oder den mutmasslichen Verstoss zu überprüfen; ausserdem muss vermerkt werden, dass es sich bei den Angaben zum Sachverhalt um Behauptungen handelt. Die meldende Person erhält über einen Zugangscode Einsicht in die Meldung und kann diese unter Benutzung des Zugangscodes ergänzen oder Änderungen verlangen.

Hat die meldende Person verlangt, anonym zu bleiben, erscheint ihr Name nicht in der Meldung.

So rasch als möglich, spätestens jedoch innerhalb von fünf Werktagen nach Erhalt der Meldung, leitet Securitas eine Untersuchung der Beschwerde oder des mutmasslichen Verstosses ein. Die Beschwerden werden einer mit der Untersuchung beauftragten Person («**Zuständiger Untersucher**») entsprechend dem Verfahrensablauf zugewiesen, der in Anhang 1 festgelegt ist.

Der Leiter CSR der Gruppe ist für die ordnungsgemässe Verwaltung des Untersuchungssystems verantwortlich, doch die Untersuchungen werden auf verschiedenen Stufen innerhalb der Gruppe von Zuständigen Untersuchern durchgeführt. Betrifft die Meldung den Leiter CSR selbst oder dessen direkten Vorgesetzten, befasst sich der Leiter der Rechtsabteilung der Gruppe damit, der in diesem Fall für die Koordination und Leitung der Untersuchung verantwortlich ist.

### 3.3 Informationen für die gemeldete Person

Der Zuständige Untersucher informiert die gemeldete Person so rasch als möglich nach Erhalt der Meldung, sofern kein erhebliches Risiko besteht, dass die Benachrichtigung der gemeldeten Person die Möglichkeit von Securitas gefährdet, die Beschwerde oder den mutmasslichen Verstoss wirksam zu untersuchen oder die notwen-

digen Beweise zusammenzutragen. Der gemeldeten Person wird Folgendes mitgeteilt: Sachverhalt, der ihr zur Last gelegt wird; Personen, welche die Meldung erhalten werden; Tatsache, dass Securitas für die Bearbeitung von Personendaten im Zusammenhang mit dieser Weisung verantwortlich ist; und Möglichkeit der gemeldeten Person, ihr Einsichts- und Berichtigungsrecht auszuüben. Nicht mitgeteilt wird ihr die Identität der meldenden Person.

Kann die gemeldete Person aufgrund des oben erwähnten Risikos nicht unverzüglich informiert werden, informiert Securitas sie, sobald dieses Risiko nicht mehr besteht und auf jeden Fall spätestens zum Zeitpunkt, der in den anwendbaren Rechtsvorschriften vorgeschrieben ist. Der Zuständige Untersucher, der mit der Meldung befasst ist, klärt auf jeden Fall ab, ob die Information der gemeldeten Person möglich und ratsam ist. Bei dieser Beurteilung werden weitere Massnahmen berücksichtigt, mit denen sich die Einwände gegen die unverzügliche Information der gemeldeten Person entkräften lassen, insbesondere technische und organisatorische Massnahmen, die getroffen werden können, um die Vernichtung von Beweisen zu verhindern.

Nachdem die gemeldete Person über das Vorliegen einer Meldung informiert wurde, wird mit ihr ein Gespräch geführt, damit sie den Sachverhalt, auf den sich die Meldung bezieht, aus ihrer Sicht darlegen kann. Der gemeldeten Person, die über das Vorliegen einer Meldung informiert wurde, wird auch so rasch als möglich mitgeteilt, ob sie während der weiteren Untersuchung der Beschwerde oder des mutmasslichen Verstosses suspendiert wird (falls dies nach dem geltenden Recht zulässig ist und als angemessen erachtet wird).

Nach Abschluss der Untersuchung ist Securitas bestrebt, innerhalb von zwei (2) Monaten zu entscheiden, welche Massnahmen getroffen werden. Sobald dieser Entscheid vorliegt, wird der gemeldeten Person mitgeteilt, ob und welche Massnahmen als Folge der Meldung getroffen werden. Wird der gemeldeten Person mitgeteilt, dass keine Massnahmen getroffen werden, endet eine (allfällige) Suspendierung dieser Person an diesem Datum automatisch.

## **4 Verfahren für Meldungen, die nicht elektronisch und systematisch bearbeitet werden**

### **4.1 Meldungen ausserhalb der Securitas Integrity Line**

Eine Beschwerde ausserhalb der Integrity Linie und der üblichen Meldekanäle kann Securitas wie folgt offen oder anonym eingereicht werden:

- per Telefon, E-Mail, Post oder persönlich an eine Führungskraft, eine Ansprechperson in der Personal- oder Rechtsabteilung oder einen Risikomanager vor Ort;
- per Telefon, E-Mail, Post oder persönlich bei der Gruppe an einen Divisions- oder Regionalleiter, an eine Ansprechperson in der Personalabteilung einer Division oder an eine Ansprechperson in der Rechtsabteilung oder einen Risikomanager einer Division oder Region;
- per E-Mail an die folgende Adresse: [integrity@securitas.com](mailto:integrity@securitas.com);
- per Post an den Leiter CSR der Gruppe: Group CSR Officer, P.O. Box 12307, S-102 28 Stockholm, Sweden.



## 4.2 Informationen für die meldende Person

Gibt die meldende Person an, dass sie anonym bleiben möchte, weist Securitas sie darauf hin, dass es bei einer anonymen Meldung schwierig sein kann, die Beschwerde oder den mutmasslichen Verstoss zu untersuchen. In einigen Ländern lassen die lokalen Vorschriften keine anonyme Meldung zu.

Securitas erstellt einen schriftlichen Bericht. Im Bericht wird das Datum aufgeführt, an dem die meldende Person die Beschwerde eingereicht oder den mutmasslichen Verstoss gegen den Kodex gemeldet hat. Sofern die lokalen Gesetze und Vorschriften nichts anderes zulassen, enthält der Bericht nur jene Informationen, die unbedingt und objektiv notwendig sind, um die Beschwerde oder den mutmasslichen Verstoss zu überprüfen, sowie den Vermerk, dass es sich bei den Angaben zum Sachverhalt um Behauptungen handelt. Die meldende Person kann die Meldung ergänzen und Änderungen verlangen.

Hat die meldende Person verlangt, anonym zu bleiben, erscheint ihr Name nicht in der Meldung.

So rasch als möglich, spätestens jedoch innerhalb von fünf Werktagen nach Erhalt der Meldung, leitet Securitas eine Untersuchung der Beschwerde oder des mutmasslichen Verstosses ein. Die Beschwerden werden einer mit der Untersuchung beauftragten Person («**Zuständiger Untersucher**») entsprechend dem Verfahrensablauf zugewiesen, der in Anhang 1 festgelegt ist.

Der Leiter CSR der Gruppe ist für die ordnungsgemässe Verwaltung des Untersuchungssystems verantwortlich, doch die Untersuchungen werden auf verschiedenen Stufen innerhalb der Gruppe von Zuständigen Untersuchern durchgeführt. Betrifft die Meldung den Leiter CSR selbst oder dessen direkten Vorgesetzten, befasst sich der Leiter der Rechtsabteilung der Gruppe damit, der in diesem Fall für die Koordination und Leitung der Untersuchung verantwortlich ist.

Securitas ermöglicht der meldenden Person, den Status der Beschwerde oder des gemeldeten Verstosses zu prüfen und zusätzliche Informationen abzugeben oder (freiwillig) Fragen zu beantworten, die (gegebenenfalls) von den Untersuchern gestellt werden.

## 4.3 Informationen für die gemeldete Person

Der Zuständige Untersucher informiert die gemeldete Person so rasch als möglich nach Erhalt der Meldung, sofern kein erhebliches Risiko besteht, dass die Benachrichtigung der gemeldeten Person die Möglichkeit von Securitas gefährdet, die Beschwerde oder den mutmasslichen Verstoss wirksam zu untersuchen oder die notwendigen Beweise zusammenzutragen. Der gemeldeten Person wird Folgendes mitgeteilt: Sachverhalt, der ihr zur Last gelegt wird; Personen, welche die Meldung erhalten werden; Tatsache, dass Securitas für die Bearbeitung von Personendaten im Zusammenhang mit dieser Weisung verantwortlich ist; und Möglichkeit der gemeldeten Person, ihr Einsichts- und Berichtigungsrecht auszuüben. Nicht mitgeteilt wird ihr die Identität der meldenden Person.

Kann die gemeldete Person aufgrund des oben erwähnten Risikos nicht unverzüglich informiert werden, informiert Securitas sie, sobald dieses Risiko nicht mehr besteht und auf jeden Fall spätestens zum Zeitpunkt, der in den anwendbaren Rechtsvorschriften vorgeschrieben ist. Der Zuständige Untersucher, der mit der Meldung befasst ist, klärt auf jeden Fall ab, ob die Information der gemeldeten Person möglich ist. Bei dieser Beurteilung werden weitere Massnahmen berücksichtigt, mit denen sich die Einwände gegen die unverzügliche Information der gemeldeten Person entkräften lassen, insbesondere technische und organisatorische Massnahmen, die getroffen werden können, um die Vernichtung von Beweisen zu verhindern.



Nachdem die gemeldete Person über das Vorliegen einer Meldung informiert wurde, wird mit ihr ein Gespräch geführt, damit sie den Sachverhalt, auf den sich die Meldung bezieht, aus ihrer Sicht darlegen kann. Der gemeldeten Person, die über das Vorliegen einer Meldung informiert wurde, wird auch so rasch als möglich mitgeteilt, ob sie während der weiteren Untersuchung der Beschwerde oder des mutmasslichen Verstosses suspendiert wird (falls dies nach dem geltenden Recht zulässig und angemessen ist).

Nach Abschluss der Untersuchung ist Securitas unter normalen Umständen bestrebt, innerhalb von zwei (2) Monaten zu entscheiden, welche Massnahmen getroffen werden. Sobald dieser Entscheid vorliegt, wird der gemeldeten Person mitgeteilt, ob und welche Massnahmen als Folge der Meldung getroffen werden. Wird der gemeldeten Person mitgeteilt, dass keine Massnahmen getroffen werden, endet eine Suspendierung dieser Person an diesem Datum automatisch.

## **5 Schutz von Personendaten**

### **5.1 Inhaber der Datensammlung für die Securitas Integrity Line**

Für die Bearbeitung von Personendaten gemäss dieser Weisung ist Securitas AB der Inhaber der Datensammlung im Sinne der anwendbaren Datenschutzgesetzgebung. Weitere Gesellschaften der Gruppe können Inhaber der Datensammlung in Bezug auf Personendaten ihrer Mitarbeitenden sein, die im Rahmen der Securitas Integrity Line bearbeitet werden. Soweit dies nach den anwendbaren Rechtsvorschriften erforderlich ist, wurde die Bearbeitung der Personendaten den zuständigen Datenschutzbehörden gemeldet oder von diesen genehmigt. Securitas bearbeitet Personendaten gemäss dieser Weisung nur zum Zweck der Meldung von Beschwerden und/oder mutmasslichen Verstössen gegen Gesetze, Vorschriften oder gegen die Unternehmenspolitik (insbesondere gegen den Kodex).

Sofern die lokale Gesetzgebung keine umfassende Bearbeitung zulässt, beschränken sich die bearbeiteten Personendaten auf die Identität, die Funktionen und die Kontaktdaten der meldenden Person, der gemeldeten Person und aller Personen, die an der Untersuchung und Behandlung der Meldung beteiligt sind, den gemeldeten Sachverhalt, die während der Untersuchung zusammengetragenen Informationen, die Ergebnisse der Untersuchung und die Massnahmen, die im Anschluss an die Untersuchung getroffen werden.

### **5.2 Datenbearbeiter für die Securitas Integrity Line**

Der Externe Anbieter handelt im Namen von Securitas als Datenbearbeiter im Sinne der Datenschutzgesetzgebung. Zu diesem Zweck hat Securitas AB für sich selbst und im Namen der Gesellschaften der Gruppe mit dem Externen Anbieter eine Vereinbarung über die Datenbearbeitung abgeschlossen. Gemäss dieser Vereinbarung:

- (a) bearbeitet der Externe Anbieter die betreffenden Personendaten nur nach den Anweisungen von Securitas;
- (b) behandelt er die Personendaten streng vertraulich und stellt sie nur über die Kommunikationskanäle bereit, die von Securitas schriftlich angegeben werden;
- (c) trifft er geeignete technische und organisatorische Sicherheitsmassnahmen, um die Personendaten zu schützen, insbesondere Zugangskontrollen für Datenbanken, verschärfte Vertraulichkeitsvereinbarungen mit seinem Personal und einen Passwortschutz für Dateien;



- (d) räumt er Securitas das Recht ein, die von ihm getroffenen Massnahmen zu überprüfen, und unterstellt seine Datenbearbeitungsanlagen Audits, die von Securitas diesbezüglich durchgeführt werden; und
- (e) hält er sich an die Anweisungen von Securitas für die Entfernung oder Vernichtung von Personendaten und gibt auf jeden Fall das gesamte papiergestützte und elektronische Material zurück, einschliesslich von Personendaten, wenn die Vereinbarung mit Securitas beendet wird, ausser wenn Securitas den Externen Anbieter anweist, dieses Material zu vernichten; in diesem Fall bestätigt der Externe Anbieter schriftlich, dass die Vernichtung erfolgt ist.

Securitas AB kann auch Vereinbarungen mit ihren Tochtergesellschaften über die ordnungsgemässe Bearbeitung von Personendaten im Rahmen der Securitas Integrity Line abschliessen.

Der Externe Anbieter hat seinen Standort in den Vereinigten Staaten und die Daten werden auf Servern bearbeitet, die ihren Standort bis Dezember 2012 in Kanada und ab diesem Zeitpunkt im Vereinigten Königreich haben. Der Externe Anbieter hält sich an die Grundsätze des sogenannten «sicheren Hafens» (Safe Harbour Principles), die am 21. Juli 2000 vom US-Handelsministerium (U.S. Department of Commerce) veröffentlicht wurden. In der Entscheidung der Europäischen Kommission 2000/520/EG wird festgestellt, dass die Grundsätze des «sicheren Hafens» ein angemessenes Datenschutzniveau im Sinne von Artikel 25 (2) der Richtlinie 95/46/EG gewährleisten. Die Befolgung der Grundsätze des «sicheren Hafens» durch den Externen Anbieter stellt somit eine gültige Rechtsgrundlage für alle Übermittlungen von Personendaten von Securitas an den Externen Anbieter gemäss dieser Weisung dar.

### **5.3 Sicherheit**

Securitas trifft die notwendigen technischen und organisatorischen Massnahmen, um die Personendaten angemessen vor Verlust oder unbefugtem Zugriff zu schützen. Securitas hat den Externen Lieferanten angewiesen, dies ebenfalls zu tun. Diese Massnahmen umfassen Authentifizierungsverfahren und andere Mittel, die notwendig sind, um die Identität der meldenden Person zu schützen, Passwörter und Personenidentifikatoren, die Aufzeichnung des Datenzugriffs und regelmässige Überprüfungen der Log-Dateien. Für alle Personen, die an der Untersuchung und Behandlung einer Meldung beteiligt sind, gelten besondere verschärfte Sicherheits- und Vertraulichkeitspflichten. Die Personendaten können mit jeder elektronischen oder anderen Datenbearbeitungsvorrichtung erfasst werden. Diese Vorrichtungen sind unter allen Umständen ausschliesslich für die Securitas Integrity Line entsprechend den Angaben in dieser Weisung bestimmt, d. h. die Personendaten werden in allen Fällen getrennt von anderen Mitarbeiterinformationssystemen oder Mitarbeiterdateien bearbeitet.

### **5.4 Speicherung und Entfernung**

Personendaten im Zusammenhang mit Meldungen, die sich als unbegründet erwiesen haben oder die nicht in gutem Glauben erfolgt sind, werden entfernt. Ist die Entfernung aufgrund von Gesetzen oder Vorschriften erforderlich, werden Personendaten im Zusammenhang mit Meldungen und Beschwerden innerhalb von zwei (2) Monaten nach Abschluss der Überprüfungsarbeit entfernt, sofern gegen die gemeldete Person keine Disziplinar-massnahmen oder Gerichtsverfahren eingeleitet werden oder wenn die meldende Person eine Meldung nicht in gutem Glauben erstattet hat; unter diesen Umständen werden die Daten innerhalb von zwei (2) Monaten entfernt, nachdem die Disziplinar-massnahmen oder ein Gerichtsverfahren, einschliesslich einer allfälligen Berufung, abgeschlossen sind.

«Entfernt» bedeutet Vernichtung der Personendaten oder Anpassung der Personendaten in einer Weise, dass die gemeldete Person und die meldende Person nicht mehr identifiziert werden können. Die Gesellschaften der Securitas Gruppe können ihre eigenen Grundsätze für die Beibehaltung der Informationen einführen, um sicherzustellen, dass das Verfahren den lokalen Regeln und Vorschriften entspricht. Nach Ablauf der oben genannten Speicherfristen dürfen die Personendaten nur zu Archivierungs- und Statistikzwecken in Übereinstimmung mit der anwendbaren Datenschutzgesetzgebung aufbewahrt werden. Jeder Zugriff auf die Personendaten wird dann ausschliesslich auf die Systemadministratoren der Gruppe zu spezifisch festgelegten Zwecken beschränkt.

## 5.5 Transparenz

Unbeschadet der sonstigen Informationserfordernisse nach dieser Weisung:

- (a) wird diese Weisung, soweit angemessen oder von Gesetzes wegen erforderlich, in eine oder mehrere der lokalen Amtssprachen übersetzt. Bei Bedarf ist das betreffende Land für diese Übersetzungen verantwortlich;
- (b) wird diese Weisung auf der Website der Integrity Line, auf My Securitas oder durch andere Mittel bereitgestellt, über die ihr Inhalt für die Mitarbeitenden einfach zugänglich ist; und
- (c) werden die Mitarbeitenden über Folgendes informiert:
  - (i) das Bestehen, die Zwecke und die Funktionsweise dieser Weisung;
  - (ii) die Identität des verantwortlichen Unternehmens von Securitas;
  - (iii) die Empfänger der Meldungen;
  - (iv) die Rechte einer gemeldeten Person auf Einsichtnahme, Berichtigung und Entfernung von Personendaten, die sie betreffen;
  - (v) jeden Export ihrer Personendaten, soweit dies nach den anwendbaren Rechtsvorschriften erforderlich ist;
  - (vi) das Recht einer Person, gegen die Bearbeitung von Personendaten, die sie betreffen, Einspruch zu erheben;
  - (vii) die Tatsache, dass die Identität der meldenden Person vertraulich bleibt, ausser wenn die Offenlegung der Identität für die Untersuchung der Beschwerde oder des mutmasslichen Verstosses oder für spätere Gerichtsverfahren unabdingbar ist, wenn sie nach den anwendbaren Rechtsvorschriften oder wegen eines wichtigen öffentlichen Interesses erforderlich ist oder wenn die Meldung nicht in gutem Glauben erfolgt ist;
  - (viii) die Tatsache, dass ein Missbrauch der Meldeverfahren, die in dieser Weisung festgelegt sind, geahndet werden kann; und
  - (ix) die Tatsache, dass eine in gutem Glauben erstattete Meldung nicht geahndet wird.

## 5.6 Einsichts-/Berichtigungs-/Entfernungsrechte

Jeder Mitarbeiter kann den Leiter CSR der Gruppe jederzeit um eine Bestätigung ersuchen, ob gegen ihn eine Beschwerde eingereicht oder ein Verstoss gemeldet wurde. Ist dies der Fall, erhält er eine vollständige schriftliche Übersicht zu den Personendaten, die über ihn verfügbar sind, ausser wenn dies:

- (a) die Untersuchung erheblich behindern würde; in diesem Fall wird eine vollständige schriftliche Übersicht abgegeben, sobald die Beweissicherung erfolgt ist; oder
- (b) die Interessen der meldenden Person oder die Rechte und Freiheiten Dritter gefährden würde; in diesem Fall enthält die schriftliche Übersicht nur Personendaten, die diese Interessen oder Rechte nicht gefährden.



Falls sich die Personendaten, die gemäss dem ersten Absatz abgegeben werden, als unrichtig oder gegenstandslos erweisen, kann die gemeldete Person die Berichtigung oder Entfernung solcher Informationen verlangen. Zudem hat die gemeldete Person das Recht, gestützt auf zwingende rechtmässige Gründe im Zusammenhang mit ihrer besonderen Situation Einspruch gegen die Bearbeitung von Personendaten in Verbindung mit einer Meldung zu erheben, sofern die Bearbeitung nicht aufgrund einer gesetzlichen Pflicht rechtmässig ist.

Die in diesem Abschnitt erwähnten Ersuchen werden so rasch als möglich beantwortet. Ein im ersten Absatz erwähntes Ersuchen wird auf jeden Fall innerhalb von vier (4) Wochen nach Erhalt beantwortet und ein im zweiten Absatz erwähntes Ersuchen wird innerhalb von zehn (10) Tagen nach Erhalt beantwortet. Jeder ablehnende Bescheid wird schriftlich und unter Angabe der Gründe mitgeteilt.

### **5.7 Bekanntgabe gegenüber Dritten ausserhalb des EWR**

Müssen Personendaten an eine natürliche oder juristische Person in einem Land ausserhalb des EWR bekanntgegeben werden, das kein angemessenes Schutzniveau im Sinne der Datenschutzrichtlinie der EU gewährleistet, werden die Anforderungen der anwendbaren Rechtsvorschriften eingehalten, die für die Übermittlung von Personendaten ins Ausland gelten.

## **6 Erlass und Änderungen der Weisung**

Diese Weisung wurde von Securitas AB erlassen, um Beschwerden und Verstösse gegen Gesetze, Vorschriften und gegen die Unternehmenspolitik (einschliesslich des Kodex) zu verhindern, aufzudecken und zu beheben, und wurde von Securitas umgesetzt.

Securitas kann diese Weisung von Zeit zu Zeit ohne vorgängige Ankündigung ändern.