Directive de Securitas AB en matière d'alertes relatives à l'intégrité

Traitement des réclamations ayant trait à de possibles violations des directives de Securitas AB (y compris du Code de valeurs et de l'éthique de Securitas AB)

Remarques liminaires : Cette Directive est établie pour toutes les sociétés du Groupe **Securitas AB** dans le monde (ci-après « Securitas » – qui n'a aucun lien de parenté avec la société suisse du même nom), représenté en Suisse par **Protectas SA** ainsi que toutes ses succursales et ses filiales.

De même, les termes utilisés pour désigner des personnes et des fonctions s'appliquent à l'ensemble des collaboratrices et des collaborateurs, nos partenaires ou d'autres parties prenantes. De ce fait et dans l'unique but de faciliter la lecture, ces termes sont utilisés au sens générique; ils ont à la fois valeur d'un féminin et d'un masculin.

1 Introduction

Le Code de valeurs et de l'éthique de Securitas AB (ci-après le « **Code** ») expose certains principes directeurs d'éthique commerciale dont Securitas attend de ses collaborateurs l'adhésion et l'application à tout moment. L'objectif de la présente Directive de Securitas AB en matière d'alertes relatives à l'intégrité (la « **Directive** » respectivement « **Securitas** ») consiste à définir le cadre principal pour le signalement et la gestion de toute réclamation concernant une violation du Code formulée par des collaborateurs ou des parties tierces contre un employé ou un membre du conseil d'administration de Securitas.
La présente Directive est soumise aux lois en vigueur. Si ses termes prévoient, en comparaison avec la législation applicable, des garanties, des droits ou des recours supplémentaires ou plus étendus pour les collaborateurs, c'est cette Directive qui s'applique. Etant donné que les pays dans lesquels Securitas est implantée ont des règles et des réglementations considérablement différentes en matière de traitement des données et d'intégrité (ce constat s'applique également à d'autres domaines pertinents), les filiales de Securitas peuvent adopter des directives locales complémentaires qui mentionnent les écarts nécessaires par rapport à la présente Directive en raison de réglementations locales. Le Représentant RSE du Groupe (RSE signifie « responsabilité sociale de l'entreprise » – de l'anglais CSR « Social Corporate Responsibility ») doit les approuver.

Securitas AB est responsable de l'ensemble du Code de valeurs et de l'éthique de Securitas ainsi que du traitement des données effectué dans le cadre du système Securitas Integrity Line. Cependant, la responsabilité ultime incombe à chaque pays qui autorise le traitement des données de ses collaborateurs dans le système. Securitas AB et les entités juridiques locales ainsi que le Fournisseur externe (comme défini ci-dessous) ont signé des contrats relatifs au traitement des données. Ceux-ci règlent les relations entre les parties à ce sujet.
La Directive s'applique à toutes les entités du Groupe Securitas qui ont mis en place le système Securitas Integrity Line et ce, à compter de la date de son implémentation. Elle n'est pas applicable à la région nord-américaine soumise actuellement à un système distinct.

2 Champ d'application

Securitas encourage tous ses collaborateurs à signaler les incidents ou les actes non conformes se rapportant à une violation potentielle de lois, de règlements ou de directives de l'entreprise (y compris du Code).
Il existe plusieurs manières de signaler des violations. La plus courante d'entre elles consiste à prévenir – au niveau local – un directeur, un représentant des ressources humaines ou le legal/risk manager. En vue de faciliter les signalements dans des situations plus délicates, Securitas a, en outre, mis en place la Securitas Integrity Line. Il s'agit d'un système de gestion de la conformité fondé sur Internet et exploité par un fournisseur tiers. Securitas gère le système Securitas Integrity Line, dans le respect des règles de la présente Directive, afin de garantir l'intégrité du système et de protéger les informations communiquées.

En raison de la législation locale en matière de protection des données (entre autres), tous les cas ne peuvent pas être signalés via le système Securitas Integrity Line. Pour assurer le traitement de tels cas, Securitas exploite également un système sur support papier permettant de formuler et de traiter des réclamations comme décrit dans le présent document. Ce système suit les mêmes principes que la version électronique de Securitas Integrity Line hormis le traitement et la systématisation électroniques de données et vise à atteindre le même degré d'intégrité et de responsabilité.

Dans certains pays, le signalement via le système Securitas Integrity Line doit se limiter à des incidents présumés ou suspectés impliquant la direction ou des collaborateurs-clé de Securitas, à savoir des directeurs de Securitas occupant au moins la fonction de chef de département ou chef de service (ou son équivalent au niveau local). Pour les pays qui appliquent ces restrictions, les incidents concernant des personnes occupant un poste hiérarchiquement moins élevé au sein de Securitas ne doivent pas être signalés via le système Securitas Integrity Line mais via des canaux de signalement internes ordinaires ou sur support papier.
Securitas garantit que les personnes signalant de bonne foi des incidents ne subiront ni représailles ni d'autres conséquences négatives.
Securitas encourage toute forme de signalements ayant trait à un non-respect de ses directives. Dans les pays où la loi l'exige, le système Securitas Integrity Line ne peut être utilisé qu'en dernier recours, c'est-à-dire, lorsque qu'aucun autre moyen ne permet de résoudre le cas. D'autres pays qui ont des réglementations et des traditions différentes privilégient cette méthode de signalement. Le fait de procéder à des signalements via le système Securitas Integrity Line est toujours une démarche volontaire et sert de complément aux canaux de signalement ordinaires.

3 Procédure pour les signalements effectués par voie électronique

3.1 Signalements via le système Securitas Integrity Line

Une réclamation peut être formulée de manière anonyme ou non auprès du fournisseur tiers du système de signalement (le « **Fournisseur externe** ») désigné par Securitas, comme suit :

(i) Par téléphone via les numéros du système Securitas Integrity Line indiqués sur le site Internet.
(ii) Via Internet à l'adresse www.securitasintegrity.com

3.2 Auteur du signalement : statut et informations qui lui sont destinés

Lorsqu'une personne effectue un signalement (ci-après désignée comme « auteur du signalement ») via le système Securitas Integrity Line, certaines informations peuvent lui être communiquées. Il se peut que les messages diffèrent localement dans un pays donné. Si tel est le cas, ces différences devraient être notifiées au Représentant RSE du Groupe avant d'être appliquées.
Si l'auteur du signalement indique qu'il souhaite rester anonyme, le Fournisseur externe ou les messages du système Securitas Integrity Line l'informeront du fait que l'anonymat peut compliquer la tenue d'une enquête détaillée sur la réclamation ou la violation alléguée. Les réglementations locales de certains pays n'autorisent pas l'anonymat.

Si l'auteur du signalement insiste sur le fait que son anonymat doit être préservé vis-à-vis de Securitas, et que la loi locale ne l'interdit pas, le Fournisseur externe peut révéler son identité à Securitas ou à une tierce partie uniquement :

(a) si une telle mesure est nécessaire à l'enquête sur la réclamation ou la violation alléguée ou à des procédures judiciaires ultérieures et si l'auteur du signalement a consenti au préalable à ce que son identité soit révélée, ou
(b) si la loi ou un intérêt public prépondérant l'exige.

Le système Securitas Integrity Line fournira à l'auteur du signalement des moyens lui permettant de vérifier le statut de sa réclamation ou de la violation qu'il a signalée ainsi que de donner des informations supplémentaires ou, le cas échéant, de répondre volontairement aux questions des enquêteurs.
Si les signalements ont lieu par téléphone, le Fournisseur externe retranscrira la conversation et déposera un rapport dans le système Securitas Integrity Line. Le rapport mentionnera la date à laquelle le collaborateur a formulé sa réclamation ou signalé une violation alléguée du Code.
Sauf disposition contraire figurant dans des lois ou des réglementations locales, le rapport ne doit contenir que des informations strictement et objectivement nécessaires pour vérifier la réclamation ou la violation alléguée et indiquera qu'il s'agit d'allégations de fait. L'auteur du signalement aura accès au rapport au moyen d'un code de connexion et sera autorisé, en utilisant ce code de connexion, à compléter le rapport ou à demander à ce qu'il soit modifié.

Si l'auteur du signalement a demandé à rester anonyme, le rapport ne citera pas son nom.
Securitas ouvrira une enquête sur la réclamation ou la violation alléguée dès que possible mais au plus tard dans les cinq jours ouvrables suivant la réception du rapport. Les réclamations seront attribuées à un enquêteur désigné (l'« **Enquêteur désigné** »), conformément au processus d'intervention par paliers décrit dans l'Annexe 1.
Le Représentant RSE du Groupe est chargé de veiller à ce que le système d'enquêtes soit géré correctement. Toutefois, il incombe aux Enquêteurs désignés de mener les enquêtes à différents niveaux du Groupe. Si le rapport concerne le Représentant RSE lui-même ou son supérieur hiérarchique direct, il est du ressort du Directeur juridique du Groupe de gérer le rapport. Il devra ensuite coordonner et diriger l'enquête.

3.3 Informations destinées à la personne concernée par le signalement

L'Enquêteur désigné informera la personne concernée par le signalement dès que possible après la réception du rapport à moins qu'il existe un risque substantiel que cette notification nuise à la capacité de Securitas d'enquêter avec efficacité sur la réclamation ou la violation alléguée ou de recueillir les preuves nécessaires. La personne concernée par le signalement sera ensuite informée des éléments suivants : les faits reprochés, le nom des desti-

nataires du rapport, le fait que Securitas est responsable du traitement de données personnelles dans le cadre de la présente Directive et la manière d'exercer son droit de consultation et de rectification. Toutefois, l'identité de l'auteur du signalement ne lui sera pas communiquée.
Si la personne concernée par le signalement ne peut pas être informée immédiatement en raison du risque mentionné ci-dessus, Securitas la préviendra dès que ce risque aura disparu et, dans tous les cas, dans les délais fixés par les lois en vigueur. L'Enquêteur désigné en charge du rapport évaluera, dans tous les cas, s'il est possible et recommandé d'informer la personne concernée par le signalement. Son évaluation tiendra compte d'autres mesures susceptibles de lever les objections formulées contre une notification immédiate à la personne concernée par le signalement, incluant, sans s'y limiter, des mesures organisationnelles et techniques pouvant être prises afin de prévenir la destruction de preuves.

Une fois que la personne concernée par le signalement a été informée, elle sera interrogée afin de lui permettre de donner son point de vue sur les faits sur lesquels le rapport est fondé. En outre, elle se verra notifier, dès que possible, si elle fait ou non l'objet d'une suspension (si les lois applicables autorisent une telle mesure et si celle-ci est jugée appropriée) pendant la suite de l'enquête sur la réclamation ou la violation alléguée.
Après conclusion de l'enquête, Securitas cherchera à déterminer les mesures à prendre dans un délai de deux mois. Une fois la décision prise, la personne concernée par le signalement sera informée des éventuelles mesures qui seront prises à la suite du rapport. Si aucune mesure n'est prise à son encontre, une éventuelle suspension prendra automatiquement fin à cette date.

4 Procédure pour les signalements non effectués par voie électronique et systématique

4.1 Signalements effectués en dehors du système Securitas Integrity Line

Une personne peut formuler auprès de Securitas une réclamation de manière anonyme ou non en ne recourant ni au système Securitas Integrity Line ni aux canaux de signalement ordinaires, mais en procédant comme suit :

- par téléphone, courrier électronique ou postal ou en se présentant en personne à un responsable local, un représentant RH ou un legal/risk manager local ;

- par téléphone, courrier électronique ou postal ou en se présentant en personne à un responsable de division ou régional du Groupe, un représentant RH de division ou un legal/risk manager de division ou régional du Groupe ;

- par courrier électronique à l'adresse suivante : integrity@securitas.com

- par courrier postal à l'adresse du Représentant RSE du Groupe comme suit : Group CSR Officer, Securitas AB, P.O. Box 12307, S-102 28 Stockholm, Suède

4.2 Informations destinées à l'auteur du signalement

Si l'auteur du signalement indique qu'il souhaite rester anonyme, Securitas l'informera du fait que l'anonymat peut compliquer la tenue d'une enquête sur la réclamation ou la violation alléguée. Les réglementations locales de certains pays n'autorisent pas l'anonymat.
Securitas établira un rapport écrit. Celui-ci mentionnera la date à laquelle l'auteur du signalement a formulé sa réclamation ou signalé une violation alléguée du Code. Sauf disposition contraire figurant dans des lois ou des réglementations locales, le rapport ne doit contenir que des informations strictement et objectivement nécessaires pour vérifier la réclamation ou la violation alléguée et indiquera qu'il s'agit d'allégations de fait. L'auteur du signalement sera autorisé à compléter le rapport ou à demander à ce qu'il soit modifié.

Si l'auteur du signalement a demandé à rester anonyme, le rapport ne citera pas son nom.
Securitas ouvrira une enquête sur la réclamation ou la violation alléguée dès que possible mais au plus tard dans les cinq jours ouvrables suivant la réception du rapport. Les réclamations seront attribuées à un enquêteur désigné (l'« **Enquêteur désigné** »), conformément au processus d'intervention par paliers décrit dans l'Annexe 1.

Le Représentant RSE du Groupe est chargé de veiller à ce que le système d'enquêtes soit géré correctement. Toutefois, il incombe aux Enquêteurs désignés de mener les enquêtes à différents niveaux du Groupe. Si le rapport concerne le Représentant RSE lui-même ou son supérieur hiérarchique direct, il est du ressort du Directeur juridique du Groupe de gérer le rapport. Il devra ensuite coordonner et diriger l'enquête.

Securitas fournira à l'auteur du signalement des moyens lui permettant de vérifier le statut de sa réclamation ou de la violation qu'il a signalée ainsi que de donner des informations supplémentaires ou, le cas échéant, de répondre volontairement aux questions des enquêteurs.

4.3 Informations destinées à la personne concernée par le signalement

L'Enquêteur désigné informera la personne concernée par le signalement dès que possible après la réception du rapport à moins qu'il existe un risque substantiel que cette notification nuise à la capacité de Securitas d'enquêter avec efficacité sur la réclamation ou la violation alléguée ou de recueillir les preuves nécessaires. La personne concernée par le signalement sera ensuite informée des éléments suivants : les faits reprochés, le nom des destinataires du rapport, le fait que Securitas est responsable du traitement de données personnelles dans le cadre de la présente Directive et la manière d'exercer son droit de consultation et de rectification. Toutefois, l'identité de l'auteur du signalement ne lui sera pas communiquée.

Si la personne concernée par le signalement ne peut pas être informée immédiatement en raison du risque mentionné ci-dessus, Securitas la préviendra dès que ce risque aura disparu et, dans tous les cas, dans les délais fixés par les lois en vigueur. L'Enquêteur désigné en charge du rapport évaluera, dans tous les cas, s'il est possible et recommandé d'informer la personne concernée par le signalement. Son évaluation tiendra compte d'autres mesures susceptibles de lever les objections formulées contre une notification immédiate à la personne concernée par le signalement, incluant sans s'y limiter des mesures organisationnelles et techniques pouvant être prises afin de prévenir la destruction de preuves.
Une fois que la personne concernée par le signalement a été informée, elle sera interrogée afin de lui permettre de donner son point de vue sur les faits sur lesquels le rapport est fondé. En outre, elle se verra notifier, dès que possible, si elle fait ou non l'objet d'une suspension (si les lois applicables autorisent une telle mesure et si celle-ci est jugée appropriée) pendant la suite de l'enquête sur la réclamation ou la violation alléguée.

Après conclusion de l'enquête et en présence de circonstances normales, Securitas cherchera à déterminer les mesures à prendre dans un délai de deux mois. Une fois la décision prise, la personne concernée par le signalement sera informée des éventuelles mesures qui seront prises à la suite du rapport. Si aucune mesure n'est prise à son encontre, une éventuelle suspension prendra automatiquement fin à cette date.

5 Protection des données personnelles

5.1 Contrôleur ou maître du fichier des données pour le système Securitas Integrity Line

Securitas AB est le contrôleur, respectivement le maître, du fichier des données, au sens des lois sur la protection des données en vigueur, pour le traitement de données personnelles conformément à la présente Directive. D'autres entreprises du Groupe peuvent exercer cette fonction pour les données personnelles de leurs collaborateurs qui sont traitées dans le système Securitas Integrity Line. Si les lois en vigueur l'exigent, les autorités compétentes en matière de protection des données ont été averties du traitement de données personnelles ou l'ont autorisé.
Securitas traitera des données personnelles conformément à la présente Directive dans l'unique but de signaler des réclamations et/ou des violations alléguées de lois, de réglementations ou de directives de l'entreprise (incluant sans s'y limiter le Code).

Sauf dispositions contraires dans les lois locales relatives à un traitement étendu des données personnelles, les données personnelles traitées seront limitées à l'identification, aux fonctions et aux coordonnées de l'auteur du signalement, de celle concernée par le signalement et de toutes les personnes participant à l'enquête et le traitement du rapport, aux faits signalés, aux informations récoltées pendant l'enquête, aux résultats de cette dernière et aux mesures qui seront prises à sa suite.

5.2 Sous-traitant chargé du traitement des données pour le système Securitas Integrity Line

Le Fournisseur externe agit en tant que sous-traitant chargé du traitement des données au nom de Securitas et au sens des lois sur la protection des données. A cette fin, Securitas AB a conclu, pour elle-même et au nom des entreprises du groupe, un contrat relatif au traitement des données avec le Fournisseur externe. Conformément à ce contrat, le Fournisseur externe :

(a) ne traite les données personnelles concernées que conformément aux instructions de Securitas ;
(b) garde les données personnelles de manière strictement confidentielle et ne les transmet que via les canaux de communication spécifiés par écrit par Securitas ;
(c) prend les mesures de sécurité techniques et organisationnelles adéquates en vue de protéger les données personnelles, incluant sans s'y limiter le contrôle d'accès aux banques de données, la signature de conventions de confidentialité renforcées avec son personnel et la protection des fichiers au moyen de mots de passe ;
(d) donne à Securitas le droit d'examiner les mesures qu'il a prises et de soumettre ses installations de traitement des données à des audits menés par Securitas en lien avec le traitement de ces données ;
(e) se conforme aux instructions de Securitas en matière de retrait ou de destruction de données personnelles et doit, dans tous les cas, restituer tous les supports papier et électroniques contenant des données personnelle à la fin du contrat avec Securitas à moins que Securitas ne lui ordonne de les détruire. Si tel est le cas, le Fournisseur externe est tenu de confirmer par écrit leur destruction.

Securitas AB peut également signer avec ses filiales des contrats relatifs au traitement correct de données personnelles dans le système Securitas Integrity Line.

Le Fournisseur externe se trouve aux Etats-Unis d'Amérique. Les données sont traitées sur des serveurs au Canada jusqu'en décembre 2012. Leur traitement aura lieu ensuite depuis le Royaume-Uni. Le Fournisseur externe adhère aux principes de la « sphère de sécurité » (Safe Harbour Principles) publiés par le Département du commerce des États-Unis d'Amérique (U.S. Department of Commerce) le 21 juillet 2000. La Décision 2000/520/EC de la Commission des communautés européennes stipule que les principes de la « sphère de sécurité » assurent un niveau adéquat de protection des données à caractère personnel, conformément à l'art. 25(2) de la directive 95/46/CE. Dès lors, l'adhésion du Fournisseur externe à ces principes fournit une base légale valable pour tous les transferts de données personnelles de Securitas au Fournisseur externe, conformément à la présente Directive.

5.3 Sécurité

Securitas prendra les mesures techniques et organisationnelles nécessaires à une protection adéquate des données personnelles contre une perte ou un accès non autorisé. Securitas a ordonné au Fournisseur externe de faire de même. Ces mesures incluront des processus d'authentification et d'autres moyens requis pour protéger l'identité de l'auteur du signalement, des mots de passe et des identifiants personnels, des journaux d'accès aux données et l'examen régulier des fichiers journaux. Toutes les personnes participant à l'enquête et traitant le rapport seront liées par des obligations spécifiques, de confidentialité et de sécurité renforcées. Les données personnelles peuvent être collectées par tout moyen – électronique ou non de traitement des données. Dans tous les cas, ces moyens doivent être uniquement dédiés au système Securitas Integrity Line comme défini conformément à la présente Directive, c'est-à-dire les données personnelles seront, dans tous les cas, traitées séparément des autres systèmes d'information ou dossiers des collaborateurs.

5.4 Conservation et retrait

Les données personnelles se rapportant à des signalements qui ont été jugés comme étant sans fondement ou effectués de mauvaise foi seront retirées. Si une loi ou un règlement exige le retrait, les données personnelles en lien avec des signalements et des réclamations seront retirées dans les deux mois suivant la fin des travaux de vérification, à moins que des mesures disciplinaires ne soit prises ou des poursuites judiciaires engagées contre la personne concernée par le signalement ou si l'auteur du signalement n'a pas effectué ce dernier de bonne foi. Dans de tels cas, les données personnelles seront retirées dans les deux mois suivant la fin des mesures disciplinaires ou des poursuites judiciaires, y compris de tout recours.

Les termes « retrait » ou « retiré » signifient la destruction des données personnelles ou leur adaptation de sorte à ce qu'il ne soit plus possible d'identifier la personne concernée par le signalement ni l'auteur de celui-ci. Les entreprises du Groupe Securitas peuvent appliquer leurs propres principes en matière de rétention d'informations afin de garantir que la procédure soit conforme aux règles et réglementations locales. Une fois les périodes de rétention mentionnées ci-dessus terminées, les données personnelles ne peuvent être conservées qu'à des fins d'archivage et de statistiques, conformément aux lois sur la protection des données en vigueur. Seuls les administrateurs du système du Groupe auront ensuite accès aux données personnelles et ce, à des fins spécifiquement déterminées.

5.5 Transparence

Sans préjudice des exigences en matière d'information conformément à la présente Directive :

(a) la présente Directive doit être traduite dans une ou plusieurs langues officielles locales là où cette mesure est appropriée ou si la loi l'exige. Le pays concerné est responsable de ces traductions si nécessaire ;

(b) la présente Directive sera disponible sur le site Internet Integrity Line, My Securitas ou par d'autres moyens permettant aux collaborateurs d'accéder facilement à son contenu ;

(c) les collaborateurs seront informés :

- (i) de l'existence, des objectifs et du fonctionnement de la présente Directive ;
- (ii) du nom de l'entreprise Securitas responsable ;
- (iii) des destinataires des rapports ;
- (iv) des droits d'une personne concernée par le signalement à l'accès à ses données personnelles, à leur rectification et à leur retrait ;
- (v) de toute exportation de leurs données personnelles, dans la mesure où la loi en vigueur l'exige ;
- (vi) du droit d'une personne à s'opposer au traitement de ses données personnelles ;
- (vii) du fait que l'identité de la personne à l'origine du signalement restera confidentielle sauf si sa divulgation est indispensable à l'enquête sur la réclamation ou la violation alléguée ou aux procédures judiciaires subséquentes, si la loi en vigueur ou un intérêt public prépondérant l'exige ou si le signalement a été effectué de mauvaise foi ;
- (viii) du fait que les abus concernant les canaux de signalement définis dans la présente Directive peuvent être sanctionnés ;
- (ix) du fait que les faux signalements effectués de bonne foi ne seront pas punis.

5.6 Droits d'accès/de correction/de retrait

Chaque collaborateur peut, en tout temps, demander au Représentant RSE du Groupe de lui confirmer si une réclamation a été formulée ou si un signalement de violation a été effectué à son encontre. Si tel est le cas, un aperçu complet des données personnelles disponibles sur sa personne lui sera fourni par écrit à moins qu'une telle mesure :

(a) entrave sérieusement l'enquête, auquel cas un tel aperçu ne lui sera donné qu'après protection des preuves ; ou

(b) compromette les intérêts de l'auteur du signalement ou les droits et les libertés d'autres personnes, auquel cas un tel aperçu ne contiendra que les données personnelles ne compromettant ni de tels intérêts ni de tels droits.

Si des données personnelles fournies conformément au premier paragraphe s'avèrent incorrectes ou non pertinentes, la personne concernée par le signalement peut demander à ce qu'elles soient rectifiées ou retirées. En outre, elle a le droit de s'opposer au traitement des données la concernant pour des raisons impérieuses et légitimes relatives à sa situation particulière, à moins que la légitimité du traitement ne se fonde sur une obligation légale.

Il sera répondu aux demandes formulées conformément au présent paragraphe dans un délai raisonnable. Dans tous les cas, une réponse sera donnée aux requêtes selon le premier paragraphe dans les quatre (4) semaines suivant leur réception et dans les dix (10) jours pour les demandes selon le second paragraphe. Tout refus requiert la forme écrite et doit être motivé.

5.7 Divulgation à des tiers en dehors de l'EEE

S'il s'avère nécessaire de divulguer des données personnelles à une personne ou une entité juridique sise dans un pays n'appartenant pas à l'Espace économique européen (EEE) et ne garantissant pas un niveau adéquat de protection au sens de la directive de l'UE sur la protection des données, les exigences des lois applicables relatives aux transferts internationaux de données personnelles doivent être remplies.

6 Adoption et modification de la Directive

Securitas AB a adopté la présente Directive en vue de prévenir, de détecter et de corriger les réclamations ou la violation de lois, de règlements et de directives de l'entreprise (y compris le Code) et l'a mise en application. Securitas peut la modifier en tout temps, sans notification préalable.

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