SprintLink International (Switzerland) GmbH

DISPOSITIF D'ALERTE – POLITIQUE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

1. Qu'est-ce que le dispositif d'alerte (Integrity Line) T-Mobile?

T-Mobile US, Inc., dont le siège social est établi au 12920 Se 38th St., Bellevue, WA 98006, Etats-Unis et ses filiales (désignées collectivement «**T-Mobile**») parmi lesquelles SprintLink International (Switzerland) GmbH, Rutistrasse 3a, 1er étage, ch-5400 Baden, Suisse («**SprintLink**»), ont mis en place un code de conduite professionnelle (ci-après «**code**») qui montre l'engagement de T-Mobile en faveur de pratiques commerciales éthiques.

Tous les employés de T-Mobile sont tenus d'agir conformément aux dispositions du code et il est de leur devoir de se faire entendre et de signaler toute infraction aux politiques de T-Mobile, au code ou encore à toute loi ou réglementation. Le dispositif d'alerte (Integrity Line) est l'un des moyens permettant aux employés ou aux tiers intéressés de faire part de toute inquiétude éventuelle ou de solliciter des conseils sur la marche à suivre s'ils pensent qu'il y a infraction ou que quelque chose ne va pas.

2. Qui est responsable du traitement des données?

SprintLink est le responsable du traitement des données liées au dispositif d'alerte (Integrity Line). Le délégué à la protection des données de SprintLink peut être contacté à l'adresse suivante: privacy@t-mobile.com.

3. Quel type de signalement peut être effectué via le dispositif d'alerte?

Si vous suspectez une infraction au code, vous devez en informer votre supérieur hiérarchique direct ou votre responsable local. Si cette démarche vous met mal à l'aise ou si vous avez l'impression que votre signalement n'a pas fait l'objet d'un traitement adéquat, vous pouvez faire part de vos inquiétudes concernant l'un des sujets énumérés ci-dessous via le dispositif d'alerte, comme indiqué au paragraphe 4 ci-après.

Vous pouvez signaler les infractions suivantes («**sujets couverts**»), qu'elles soient avérées ou présumées. Notez toutefois que seules doivent être signalées les inquiétudes relevant des sujets couverts énumérés ci-après et concernant les activités commerciales de SprintLink, non des affaires privées (c'est-à-dire qui ne concernent pas la relation de travail d'un employé):

(1) l'enregistrement délibéré, malhonnête ou discutable de registres ou rapports financiers et comptables; (2) l'acceptation de cadeaux ou d'argent de la part de prestataires, fournisseurs, concessionnaires, tiers ou fonctionnaires (ou à l'inverse la remise de cadeaux ou d'argent à ces derniers) dans l'intention d'exercer abusivement une quelconque influence; (3) les infractions ou le non-respect de toute règle, réglementation ou loi; (4) les circonstances dans lesquelles les actes d'un employé ou de quelqu'un d'autre engendrent une situation dans laquelle le devoir de loyauté de l'employé envers T-Mobile ou sa capacité à agir dans le meilleur intérêt de l'entreprise est compromis; (5) l'accès non autorisé aux informations confidentielles d'un client, leur divulgation ou leur utilisation abusive; (6) le refus de droits et privilèges normaux en raison de l'appartenance à un groupe discriminé; (7) l'accès non autorisé aux informations confidentielles d'un employé, leur divulgation ou leur utilisation abusive; (8) toute situation impliquant le stockage, la manipulation ou l'élimination inadéquats de matières ou déchets dangereux ou le non-respect des politiques environnementales de l'entreprise; (9) la tromperie délibérée pour en tirer un profit injuste ou illicite; (10) tout comportement inopportun, intimidant, hostile ou abusif en raison de l'appartenance d'un individu à un groupe discriminé; (11) le non-respect d'une politique, loi ou réglementation ayant des conséquences néfastes

sur la santé ou la sécurité des employés de T-Mobile, ses partenaires commerciaux, ses concessionnaires ou clients; (12) toute forme de représailles à l'encontre d'un individu qui s'est opposé à une pratique illicite ou qui a porté des accusations, a témoigné, a contribué ou participé à une enquête; (13) toute action ou situation ayant des répercussions sur la sécurité des employés, concessionnaires, partenaires commerciaux ou clients; (14) toutes avances sexuelles non sollicitées ou offensantes ainsi que tout acte ou toute remarque offensante d'ordre sexuel; (15) tout accès non autorisé à des informations confidentielles de T-Mobile, leur divulgation ou leur utilisation abusive; (16) les incidents liés l'accaparement d'argent, de marchandise ou de tout autre bien sans recours à la force; et (17) les circonstances dans lesquelles un employé est impliqué dans la destruction, la perte ou le gaspillage de ressources de l'entreprise par faute intentionnelle ou par négligence.

Les inquiétudes liées à d'autres sujets doivent être signalées à votre supérieur hiérarchique ou votre responsable local. Elles ne peuvent pas être signalées via le dispositif d'alerte.

4. Comment effectuer un signalement par le biais du dispositif d'alerte?

Vous pouvez signaler tout sujet couvert par le biais du dispositif d'alerte T-Mobile en contactant l'un des avocats suivants, appartenant à l'antenne zurichoise du cabinet Baker McKenzie, de la manière de votre choix:

- Boris Wenger
  - Mail: Boris.Wenger@bakermckenzie.com
  - Ligne directe: (+41) 044 384 13 42
  - Mobile: (+41) 079 900 25 53
- Roger Thomi
  - Mail: Roger.Thomi@bakermckenzie.com
  - Ligne directe: (+41) 044 384 14 91
  - Mobile: (+41) 079 514 52 48

Votre signalement sera examiné conformément aux lois de blocage et à la législation sur la protection des données en vigueur en Suisse. Le cas échéant, Baker McKenzie transmettra les signalements de sujets couverts au service Conformité et Ethique de T-Mobile pour un examen plus approfondi. Ils seront alors enregistrés dans le système de gestion de cas du dispositif d'alerte de T-Mobile, lequel est administré par un tiers: Convercent, Inc., 3858 Walnut Street, Suite #255 Denver, CO 80205, Etats-Unis («**Convercent**»).

SprintLink vous encourage expressément à effectuer votre signalement de façon strictement anonyme, sans vous identifier. Vous n'avez pas à divulguer votre identité ni aucune autre information personnelle. Soumettre anonymement un signalement n'aura aucune répercussion néfaste sur vous. SprintLink ne prendra aucune mesure disciplinaire à l'encontre d'un employé qui soumet un signalement de bonne foi. Celui-ci ne sera pas discriminé et ne fera pas l'objet de mesures de représailles. S'identifier pour soumettre un signalement tient plus de l'exception que de la règle.

5. Quelles sont les catégories de données personnelles susceptibles d'être traitées dans le cadre d'un signalement via le dispositif d'alerte?

Les données à caractère personnel relevant des catégories suivantes sont susceptibles d'être traitées:

- l'identité, le poste et les coordonnées (par ex. nom-prénom, vérification des qualifications, numéro d'identification, intitulé de poste, adresse professionnelle, numéro de téléphone et adresse mail) de l'auteur du signalement. Par conséquent, les données personnelles relatives à l'auteur du signalement ne sont traitées que si l'individu en question choisit de son plein gré, exceptionnellement, de dévoiler son identité lors du signalement;
- l'identité, le poste et les coordonnées de(s) (l')individu(s) faisant l'objet du signalement;

- l'identité, le poste et les coordonnées de(s) (l')individu(s) chargé(s) du traitement des faits signalés;
- les données à caractère personnel contenues dans (i) les faits signalés, (ii) les échanges et autres informations collectées et examinées en lien avec le signalement et l'enquête ultérieure sur les faits signalés, et dans (iii) le rapport d'enquête; et
- les données à caractère personnel contenues dans les informations se rapportant au résultat et aux conséquences de l'enquête sur les faits signalés.

Vous choisissez de votre plein gré de fournir des informations à caractère personnel en tant qu'auteur du signalement, conformément aux procédures énoncées dans le présent document. Ne pas fournir vos données à caractère personnel liées aux faits signalés peut retarder la prise en compte de votre signalement voire empêcher SprintLink d'y réagir. Quoi qu'il en soit, la décision de révéler votre identité vous appartient et choisir de rester anonyme n'aura aucune répercussion négative sur vous.

6. Quelles sont les finalités du traitement des données?

Le traitement des données à caractère personnel – qu'elles soient contenues dans les signalements effectués par le biais du dispositif d'alerte ou obtenues au moyen de toute enquête – est primordial pour mettre en œuvre le code, assurer le respect des lois en vigueur par l'entreprise et préserver l'intégrité et l'éthique dans les pratiques commerciales. Il permet d'enquêter sur le comportement signalé et d'adopter les mesures correctives nécessaires que l'enquête aura fait ressortir, comme énoncé par la présente politique de confidentialité.

7. Quelles sont les bases juridiques du traitement des données?

Les bases juridiques du traitement par SprintLink des données à caractère personnel dans le cadre du dispositif d'alerte sont les suivantes:

- Le traitement des données est nécessaire pour les intérêts légitimes poursuivis par SprintLink et/ou T-Mobile d'après une évaluation de ces derniers, ainsi que pour les intérêts ou libertés et droits fondamentaux des individus concernés. Parmi les intérêts légitimes de SprintLink et/ou T-Mobile figurent le fait d'enquêter et de prendre les mesures appropriées concernant une infraction potentielle au code sur les sujets couverts, assurant ainsi la conformité et permettant de constater, d'exercer ou de défendre un droit en justice dans ce contexte. Relèvent également des intérêts légitimes de SprintLink et T-Mobile:
  - la prévention des fraudes et fautes professionnelles en matière de comptabilité, de contrôles comptables internes, d'audits et de signalements;
  - la lutte contre la corruption, les crimes bancaires et financiers et les délits d'initié;
  - et la protection des intérêts environnementaux légitimes et des droits de l'homme.

  Ne pas poursuivre ces intérêts légitimes risquerait d'avoir de graves conséquences pour SprintLink et/ou T-Mobile.

- Il se peut que nous nous justifiions par la disposition réglementaire qui autorise le traitement des données à caractère personnel pour détecter les infractions pénales s'il existe des raisons étayées de croire qu'un employé a commis une telle infraction alors qu'il était employé par l'entreprise, que le traitement de ces données est nécessaire pour enquêter sur l'infraction, que ce dernier n'outrepasse pas les intérêts légitimes de l'employé et qu'il n'est pas disproportionné.

- En ce qui concerne l'identité de l'auteur du signalement, si ce dernier choisit de son plein gré de faire exception au signalement anonyme et de révéler son identité en soumettant son signalement, SprintLink présume son consentement au traitement de ses données à caractère personnel.

8. Qui peut utiliser le dispositif d'alerte?

Les individus tels que les employés et agents de T-Mobile et de ses filiales, les membres du conseil d'administration de T-Mobile, ses partenaires commerciaux (notamment les agents, contractuels, prestataires et fournisseurs) et autres tiers peuvent effectuer des signalements conformément au paragraphe 3 ci-dessus.

9. Les informations resteront-elles confidentielles?

Si vous choisissez (de faire exception au signalement anonyme et) de révéler votre identité en soumettant votre signalement, les données relatives à votre identité seront traitées comme suit:

l'identité d'un individu effectuant un signalement de bonne foi sera traitée de manière confidentielle dans la mesure du possible. Seules les personnes ayant expressément besoin de connaître les informations collecteront et traiteront les signalements. Ces personnes seront tenues à un devoir spécifique de confidentialité.

En principe, l'identité d'un individu effectuant un signalement de bonne foi ne sera pas divulguée à des tiers. Cependant, il existe des exceptions à ce principe notamment:

- si cette divulgation s'avère raisonnablement nécessaire pour traiter comme il se doit le signalement et/ou pour mener une enquête complémentaire et/ou prendre des mesures à la lumière de l'enquête;

- si cette divulgation s'avère légalement nécessaire (notamment si les autorités compétentes exigent de connaître l'identité de l'auteur du signalement, sous réserve que nous ayons l'obligation légale d'accéder à cette demande).

10. Les données à caractère personnel seront-elles transmises à des tiers et à l'étranger?

T-Mobile US, Inc. et Convercent sont implantées aux Etats-Unis. Selon la Commission européenne, les Etats-Unis n'offrent pas un niveau de protection des données adéquat. Les précautions suivantes seront mises en place afin de garantir que le transfert de données personnelles à T-Mobile US, Inc. et Convercent soit conforme avec les exigences de l'article 44 et suivants du RGPD et avec les dispositions de la législation suisse sur la protection des données:

- SprintLink et T-Mobile US, Inc. ont conclu un accord approprié de transfert de données basé sur les clauses contractuelles types (2004/915/CE).
- Convercent traite les données reçues par le biais du dispositif d'alerte dans le strict respect des instructions d'un accord sur le traitement des données qui inclut les clauses contractuelles types (2010/87/UE).

Vous pouvez obtenir des copies des contrats mentionnés dans ce paragraphe en envoyant un mail à l'adresse: privacy@t-mobile.com.

11. Qu'advient-il de votre signalement?

Les signalements suffisamment précis et liés à des sujets couverts seront transmis au service Conformité et Ethique de T-Mobile à des fins d'examen approfondi et d'enquête le cas échéant. Dans la mesure où c'est nécessaire, ils communiqueront le signalement à des conseillers, experts judiciaires et sociétés d'audit, le cas échéant, en fonction du sujet du signalement.

Les signalements de sujets non couverts par le dispositif d'alerte seront rejetés et supprimés, et l'auteur du signalement (si son identité est connue) sera informée qu'il doit faire part de ses inquiétudes au niveau local, car le signalement ne peut être traité par le biais du système d'alerte.

Si une faute signalée est confirmée dans le cadre d'une enquête, dans la mesure où cela est requis pour y remédier ou pour la sanctionner, le(s) supérieur(s) hiérarchique(s) des employés concernés en sera (seront) informé(s), si nécessaire, en fonction de la gravité et de la nature du signalement confirmé et, par conséquent, des procédures judiciaires telles que des plaintes pénales peuvent être engagées.

Aucune prise de décision automatique n'a lieu au cours de ce processus.

12. Communication d'informations aux employés faisant l'objet d'un signalement

Les employés seront informés dès que possible qu'ils ont fait l'objet d'un signalement après l'enregistrement de ce dernier conformément au droit applicable. Toutefois, ces informations peuvent être communiquées en différé si cela est nécessaire à des fins d'enquête ou d'autres fins de collecte de preuves.

13. Quelles sont les conséquences d'un signalement abusif?

Les signalements abusifs, notamment les signalements de mauvaise foi, peuvent entraîner des mesures disciplinaires allant jusqu'au licenciement, ainsi que des sanctions judiciaires conformément au droit du travail applicable et à toute autre règle ou réglementation applicable.

14. Conservation des informations

Toute information recueillie à la suite d'un signalement ne sera conservée qu'aussi longtemps que nécessaire et aux fins pour lesquelles elle a été recueillie, conformément au droit applicable, comme indiqué ci-dessous.

Les données à caractère personnel relatives aux signalements jugés infondés sont supprimées sans délai. Les données à caractère personnel relatives aux signalements donnant lieu à une enquête sont supprimées ou anonymisées immédiatement et généralement dans un délai de deux mois suivant la fin de l'enquête, sauf si des mesures disciplinaires ou une procédure judiciaire sont engagées (voir ci-dessus), auquel cas les données sont conservées jusqu'à la conclusion finale de telles procédures.

15. Droits relatifs aux données à caractère personnel

Tout individu (notamment les auteurs de signalements ou les personnes faisant l'objet d'un signalement) dispose de certains droits relatifs aux données personnelles traitées comme indiqué dans la présente politique. Ces droits sont résumés ci-dessous. Veuillez noter que l'exercice de ces droits est soumis à certaines exigences et conditions énoncées dans le droit applicable (par exemple, le RGPD). Ces droits peuvent également être limités par la législation locale en matière de protection des données.

Tout individu est également en droit de déposer une plainte auprès de l'autorité de contrôle concernant la protection des données.

Si vous souhaitez exercer ces droits, vous devez contacter privacy@t-mobile.com.

(i) Droit de retrait

Si un individu, en particulier l'auteur du signalement, a consenti à une quelconque activité de traitement de ses données à caractère personnel, il peut à tout moment revenir sur son consentement avec effet sur l'avenir.

(ii) Droit d'accès

Tout individu est en droit d'obtenir de SprintLink la confirmation que ses données à caractère personnel soient traitées et, le cas échéant, de demander un accès à ces données, y compris les catégories de données à caractère personnel traitées, la finalité du traitement et les destinataires ou catégories de destinataires. Tout individu peut obtenir une copie des données à caractère personnel faisant l'objet d'un traitement.

Étant donné qu'il peut être nécessaire de tenir compte des intérêts d'autrui, il ne s'agit pas d'un droit absolu et les intérêts d'autres individus peuvent restreindre le droit d'accès. Le droit d'accès ne s'applique pas, par exemple, dans le cas où cet accès divulguerait des informations qui, en vertu de la loi ou de leur nature, doivent rester confidentielles, notamment en raison d'intérêts légitimes supérieurs d'un tiers.

(iii) Droit de rectification

Tout individu est en droit de nous demander la rectification de données à caractère personnel incorrectes le concernant. Selon les finalités du traitement, tout individu peut faire compléter les données à caractère personnel incomplètes, notamment en fournissant une déclaration complémentaire.

(iv) Droit à l'effacement (droit à l'oubli)

Tout individu est en droit de demander l'effacement des données à caractère personnel le concernant.

(v) Droit de restreindre le traitement

Dans certaines circonstances, vous pouvez obtenir de notre part la restriction du traitement de vos données à caractère personnel. Dans ce cas, les données correspondantes seront marquées et nous ne pourrons les traiter qu'à certaines fins.

(vi) Droit à la portabilité des données

Tout individu est en droit de recevoir les données à caractère personnel le concernant – qu'il a fournies – dans un format structuré, couramment utilisé et lisible par machine, et de transmettre ces données à une autre entité.

(vii) Droit d'opposition

Tout individu est en droit, dans certaines circonstances, de s'opposer à tout moment, pour des raisons liées à sa situation particulière, au traitement de ses données à caractère personnel par nos soins et il peut nous être demandé de ne plus les traiter.