SprintLink France SAS

POLITIQUE DE PROTECTION DES DONNÉES POUR LE DISPOSITIF D'ALERTE

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

T-Mobile US, Inc., dont l'adresse du siège social est 12920 Se 38th St., Bellevue, WA 98006, États-Unis et ses filiales (ensemble «**T-Mobile**») comprenant SprintLink France SAS, 3-5 Rue St Georges, TMF Pole, 75009 Paris, France («**SprintLink**»), ont mis en place un Code de conduite professionnelle («**Code**») qui illustre l'engagement de T-Mobile pour des pratiques professionnelles conformes à l'éthique.

Tous les employés de T-Mobile sont tenus d'agir conformément aux principes du Code et ont le devoir de s'exprimer et de signaler toute violation du Code. Le « dispositif d'alerte » (Integrity Line) est un moyen, offert aux employés ou aux tiers intéressés, de faire part de préoccupations ou de demander des conseils sur la marche à suivre si une violation est constatée ou si quelque chose ne semble pas correct.

2. Qui est responsable du traitement des données ?

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

3. Quel type d'information peut être signalé par le biais du dispositif d'alerte ?

Si vous estimez qu'une violation du Code a été commise, vous devez signaler cette violation présumée à votre superviseur direct ou votre responsable local. Si cette démarche de signalement au niveau local vous met mal à l'aise, ou si, après votre signalement, vous ne croyez pas que votre signalement ait été transmis de manière adéquate, vous pouvez signaler vos préoccupations concernant les sujets listés ci-dessous à la société mère située aux États-Unis par le biais du dispositif d'alerte.

Les informations contenues dans les signalements que vous soumettez par le biais du dispositif d'alerte doivent uniquement être basées sur des faits et avoir un lien direct avec le sujet de votre signalement. Vous pouvez signaler des préoccupations concernant les violations avérées ou présumées suivantes («**Sujets Pertinents**») :

(1) l'enregistrement intentionnel, malhonnête ou discutable d'états, registres ou rapports comptables et financiers.

(2) le fait d'offrir ou d'accepter des cadeaux ou paiements à/de prestataires, fournisseurs, négociants, autres tiers ou représentants gouvernementaux avec l'intention d'exercer une influence négative.

(3) infractions ou délits et violations flagrantes ou non-respect évident d'une règle, réglementation ou loi,

(4) lorsque l'action d'un employé ou autre crée une situation où le devoir de loyauté de l'employé envers T-Mobile ou sa capacité à agir dans le meilleur intérêt de la société est compromis,

(5) accès non autorisé, divulgation, ou mauvaise utilisation des informations sensibles d'un client,

(6) faire obstacle aux privilèges ou droits normaux en raison de l'appartenance d'un individu à une catégorie protégée,

(7) accès non autorisé, divulgation, ou mauvaise utilisation des informations sensibles d'un employé,

(8) toute situation impliquant le stockage, la manipulation ou l'élimination non conformes de déchets ou matériaux à risque ou le non-respect des politiques de durabilité de la société,

(9) tromperie intentionnelle pour tirer un profit injuste ou illicite,

(10) comportement inopportun, intimidant, hostile ou grossier en raison de l'appartenance d'un individu à une catégorie protégée,

(11) non-respect d'une politique, loi ou réglementation ayant pour conséquence une influence néfaste sur la santé ou la sécurité des employés, partenaires commerciaux, négociants ou clients de T-Mobile,

(12) toute forme de représailles à l'encontre d'un individu car il ou elle s'est soit opposé à une pratique illicite en matière d'emploi ou a porté une accusation, témoigné, contribué ou participé à une enquête,

(13) une action ou situation ayant une influence sur la sécurité des employés, négociants, partenaires commerciaux ou clients,

(14) toutes avances sexuelles non sollicitées et offensantes ou tous actes et remarques offensantes d'ordre sexuel,

(15) accès non autorisé, divulgation ou mauvaise utilisation d'informations commerciales confidentielles et propriétaires de T-Mobile,

(16) incidents liés à la prise d'argent liquide, de marchandise ou d'autres biens sans faire usage de la force, et

(17) lorsqu'un employé est impliqué dans la destruction, perte ou gaspillage de biens appartenant à la société soit par le biais d'une faute intentionnelle ou de négligence.

Les préoccupations concernant des sujets autres que ceux listés ci-dessus doivent être transmises à votre superviseur direct ou votre responsable local et ne peuvent pas faire l'objet d'un signalement par le biais du dispositif d'alerte.

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

Vous pouvez signaler tout Sujet Pertinent par le biais du dispositif d'alerte T-Mobile à l'adresse https://www.t-mobile.com/responsibility/legal/integrity-line. Le dispositif d'alerte est géré par la société tierce Convercent, Inc., 3858 Walnut Street, Suite #255 Denver, CO 80205, États-Unis («**Convercent**»).

SprintLink vous encourage expressément à soumettre votre signalement de manière strictement anonyme et sans vous identifier. Vous n'avez aucune obligation de divulguer votre identité ou toute autre information personnelle vous concernant. Soumettre un signalement de manière anonyme n'entraînera aucune conséquence négative pour vous. SprintLink ne prendra aucune mesure disciplinaire, ne fera pas preuve de

discrimination et n'engagera pas de riposte contre un employé ayant soumis un signalement de manière anonyme en toute bonne foi. Dans la mesure où SprintLink ne pourra pas vous contacter pour le suivi d'un signalement que vous soumettez de manière anonyme, de tels signalements doivent concerner des violations graves et établies et comprendre suffisamment de faits détaillés. De tels signalements anonymes feront l'objet d'une attention particulière et une analyse préalable sera menée afin de décider du traitement de tels signalements. Cependant, SprintLink se réserve le droit de ne pas poursuivre le traitement de signalements anonymes qui ne fournissent pas suffisamment de détails ou qui ne concernent pas des violations suffisamment sérieuses.

5. Quelles catégories de données personnelles pourront être traitées en conséquence d'un signalement sur le dispositif d'alerte ?

Les catégories de données personnelles suivantes pourront être traitées :

- identité, poste et informations de contact (p.ex. prénom et nom, identifiants de vérification, numéro d'identification, intitulé du poste, adresse de travail, numéro de téléphone, adresse e-mail) de la personne soumettant un signalement. Par conséquent, toutes les données personnelles concernant la personne soumettant un signalement ne sont traitées que si la personne soumettant un signalement choisit de divulguer son identité lorsqu'il ou elle soumet le signalement ;
- l'identité, le poste et les informations de contact des personnes faisant l'objet du signalement,
- l'identité le poste et les informations de contact des personnes impliquées dans le traitement des faits signalés ;
- les données personnelles contenues dans (i) les faits signalés, (ii) les échanges et autres informations recueillies et examinées en lien avec le signalement et l'enquête en résultant concernant les faits signalés, et dans (iii) le rapport d'enquête ; et
- les données personnelles contenues dans les informations se rapportant au résultat et aux conséquences de l'enquête concernant les faits signalés.

Le fait de divulguer ses données personnelles en tant que personne soumettant un signalement conformément avec les procédures décrites dans le présent document est volontaire. Le fait de ne pas divulguer de données personnelles liées aux faits signalés peut retarder ou rendre impossible l'action de SprintLink concernant tout signalement soumis. Le fait de divulguer votre identité est dans tous les cas volontaire et il n'y a aucune conséquence négative si vous ne divulguez pas votre identité.

6. Quelles sont les finalités du traitement des données ?

Les données personnelles sont traitées de concert avec le dispositif d'alerte pour recueillir les signalements concernant de risques existants ou réels de comportement ou situations incompatibles avec le Code.

Le traitement de données personnelles présentes dans des signalements soumis par le biais du dispositif d'alerte et obtenues au cours de toute enquête est essentiel pour mettre en œuvre le Code, garantir la conformité de la société avec les lois en vigueur et respecter l'intégrité et l'éthique dans les pratiques commerciales. Il permet de conduire l'enquête concernant le comportement signalé et de prendre les mesures correctives nécessaires conséquentes à cette enquête, comme prévu par cet avis.

7. Quelles sont les bases juridiques pour le traitement des données?

Les bases juridiques pour le traitement, par SprintLink, des données personnelles liées au dispositif d'alerte sont :

- Le traitement des données est nécessaire pour les intérêts légitimes poursuivis par SprintLink et/ou T-Mobile reposant sur une évaluation des intérêts légitimes de SprintLink et/ou T-Mobile, ainsi que sur les intérêts ou droits fondamentaux et libertés des sujets concernés pour les données. Les intérêts légitimes de SprintLink et/ou T-Mobile incluent le fait d'enquêter et de prendre les mesures appropriées concernant une violation potentielle du Code des Sujets Pertinents afin d'apporter une garantie de conformité et d'établir, exercer ou défendre des revendications légales dans ce contexte. Les intérêts légitimes de SprintLink et T-Mobile incluent également :
    - la prévention des fraudes et fautes professionnelles en matière de comptabilité, de contrôles internes de comptabilité et de questions de vérification et de signalement ;
    - 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 humains.

  Le fait de ne pas poursuivre ces intérêts légitimes risque d'avoir de graves conséquences pour SprintLink et/ou T-Mobile.

8. Qui peut utiliser le dispositif d'alerte ?

Les individus, notamment les employés et agents de T-Mobile et ses filiales, les membres du conseil d'administration de T-Mobile, partenaires commerciaux (notamment les agents, contractuels, prestataires et fournisseurs) et autres tierces parties peuvent soumettre des signalements conformément à la Section 3 ci-dessus.

9. Les informations resteront-elles confidentielles ?

Si vous choisissez (à titre d'exception à la règle de signalement anonyme) de divulguer votre identité lors de la soumission d'un signalement, les données relatives à votre identité seront traitées comme décrit ci-dessous :

L'identité d'une personne soumettant 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'une personne soumettant un signalement de bonne foi ne sera pas divulguée à des tierces parties, à moins que cette personne en ait donné l'accord. Cependant, votre identité peut être divulguée aux autorités judiciaires.

10. Les données personnelles seront-elles transmises à des tierces parties et à l'étranger ?

T-Mobile US, Inc. et Convercent sont situées aux États-Unis. Selon la Commission Européenne, les États-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 en conformité avec les exigences de l'Article 44 et suivants du RGPD :

- SprintLink et T-Mobile US, Inc. ont conclu un accord approprié de transfert de données basé sur les Clauses Contractuelles Types (2004/915/EC).
- Convercent traite les données reçues par le biais du dispositif d'alerte uniquement en conformité avec les instructions d'un accord sur le traitement des données qui inclut les Clauses Contractuelles Types (2010/87/EU).

Des copies des contrats mentionnés dans cette Section sont disponibles en envoyant un courriel à l'adresse privacy@t-mobile.com.

11. Qu'adviendra-t-il de votre signalement ?

Lorsque vous aurez soumis un signalement, vous recevrez un accusé de réception récapitulant les informations que vous avez fournies et tout document joint.

Les signalements suffisamment spécifiques et liés à des Sujets Pertinents seront transmis au service Conformité et Éthique de T-Mobile pour un examen approfondi et une enquête si nécessaire. Dans la mesure où c'est nécessaire, ils partageront le signalement avec des conseillers, experts judiciaires et sociétés d'audit, le cas échéant, selon le sujet du signalement.

Les signalements qui ne correspondent pas aux Sujets Pertinents seront rejetés et supprimés, et la personne ayant soumis le signalement sera informée qu'il/elle doit soumettre ses préoccupations au niveau local, car le signalement ne peut être traité par le biais du système d'alerte.

Vous serez informé(e) lorsqu'une décision aura été prise concernant le rejet, la suppression ou le lancement d'une enquête approfondie concernant votre signalement.

Si un signalement est vérifié dans le cadre d'une enquête, dans la mesure où cela est requis pour remédier au mauvais comportement vérifié ou le sanctionner, le(s) cadre(s) hiérarchique(s) des employés concernés sera (seront) informé(s), si nécessaire, selon la gravité et la nature du signalement vérifié et, par conséquent, des procédures judiciaires telles que des plaintes pénales peuvent être engagées.

Vous serez informé(e) des mesures prises en conséquence de votre signalement telles que des modifications ou l'adoption de règles internes, des mesures organisationnelles, des mesures disciplinaires ou des procédures judiciaires.

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

12. Informations destinées aux employés faisant l'objet d'un signalement

Les employés seront informés dès que possible, dans un délai raisonnable et pas plus d'un mois, du fait qu'ils ont fait l'objet d'un signalement suite à l'enregistrement du signalement conformément à la loi en vigueur. Cependant, de telles informations peuvent être retardées si et tant que cela est nécessaire à des fins d'enquête et de collecte de preuves.

L'identité des employés faisant l'objet d'un signalement sera tenue confidentielle, jusqu'à ce que les faits du signalement aient fait l'objet d'une enquête et soient vérifiés comme étant fondés, et puissent être transmis aux autorités judiciaires.

SprintLink ne fournira pas l'identité de la personne ayant soumis un signalement ou celles des individus tiers identifiés dans le signalement aux employés faisant l'objet du signalement, à moins que cela soit nécessaire dans le cadre de mesures disciplinaires ou de procédures judiciaires.

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

Les signalements abusifs, y compris les signalements soumis de mauvaise foi, peuvent entraîner une action disciplinaire, jusqu'à et incluant la résiliation du contrat de travail, ainsi que des sanctions judiciaires conformément aux lois en vigueur en matière d'emploi et autres règles et réglementations en vigueur.

14. Rétention d'informations

Toutes informations collectées à la suite d'un signalement ne seront conservées qu'aussi longtemps que nécessaire et pour l'objectif pour lequel elles ont été collectées conformément à la loi en vigueur, comme expliqué ci-dessous.

Les données personnelles liées à des signalements ayant été établis comme non fondés seront supprimées sans délai. Les données personnelles liées à des signalements donnant suite à une enquête seront supprimées ou anonymisées rapidement et habituellement dans les 2 mois après la fin de l'enquête, à moins que des mesures disciplinaires ou des procédures judiciaires soient engagées comme indiqué ci-dessus, dans quel cas les données seront conservées jusqu'à la conclusion finale de ces procédures.

15. Droits relatifs aux Données Personnelles

Les individus (tels que les personnes soumettant un signalement ou les personnes faisant l'objet d'un signalement) ont certains droits relatifs aux données personnelles traitées comme il est décrit dans cette politique. Ces droits sont résumés ci-dessous. Il est important de remarquer que le fait d'exercer ces droits est sujet à certaines exigences et conditions telles que présentées dans la loi en vigueur (p.ex. le RGPD). Ces droits peuvent également être limités par la loi locale de protection des données.

Les individus ont aussi le 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 les individus, en particulier les personnes soumettant un signalement, ont exprimé leur consentement pour toute activité de traitement de leurs données personnelles, elles peuvent retirer leur consentement à tout moment avec effet sur l'avenir. Un tel retrait n'affectera pas le caractère licite du traitement avant le retrait du consentement.

(ii) Droit d'accès

Les individus peuvent avoir le droit d'obtenir la confirmation de SprintLink pour savoir si leurs données personnelles sont traitées et, si elles le sont, de demander un accès à ces données personnelles, y compris les catégories de données personnelles traitées, la finalité du traitement et les destinataires ou catégories de destinataires. Les individus ont le droit d'obtenir une copie des données personnelles faisant l'objet de traitement.

Du fait qu'il peut être nécessaire de prendre en considération les intérêts des autres, il ne s'agit pas d'un droit absolu et les intérêts des autres individus peuvent restreindre le droit d'accès. Le droit d'accès ne s'applique pas, par exemple, dans le cas où l'accès divulguerait des informations qui, en matière légale ou par nature, doivent être tenues secrètes, particulièrement en raison d'intérêts légitimes prioritaires d'une tierce partie.

(iii) Droit de rectification

Les individus peuvent avoir le droit d'exiger de notre part la rectification de données personnelles incorrectes les concernant. Selon les finalités du traitement, les individus peuvent avoir le droit que les données personnelles incomplètes soient complétées, notamment par la fourniture d'une déclaration complémentaire.

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

Les individus peuvent avoir le droit d'exiger l'effacement des données personnelles les concernant.

(v) Droit de restreindre le traitement

Selon certaines conditions, vous pouvez avoir le droit d'exiger de notre part la restriction du traitement de vos données personnelles. Dans ce cas, les données pertinentes seront marquées et ne pourront être traitées par nous que pour certaines finalités.

(vi) Droit à la portabilité des données

Les individus peuvent avoir le droit de recevoir les données personnelles les concernant qu'ils ont fournies dans un format structuré, couramment utilisé et lisible par machine, et peuvent avoir le droit de transmettre ces données à une autre entité.

(vii) Droit de contester

Les individus peuvent, dans certains cas, avoir le droit de contester à tout moment, sur des motifs concernant leur situation particulière, le traitement de leurs données personnelles par nous et il peut être exigé de notre part de ne plus traiter leurs données personnelles.