Sprint International Austria GmbH
DATENSCHUTZRICHTLINIE BETREFFEND DIE DATEN DER INTEGRITY LINE

1. Was versteht man unter der T-Mobile „Integrity Line“ (einer Anlaufstelle zur Meldung von Umständen, die die Integrität des Unternehmens gefährden könnten)?

T-Mobile US, Inc. mit Sitz in 12920 Se 38th St., Bellevue, WA 98006, USA und seine Tochtergesellschaften (gemeinsam „**T-Mobile**“) – zu denen auch Sprint International Austria GmbH, Wien, Börsehaus, Schottenring 16, Büro 13, 1010 Wien, Österreich zählt („**SprintLink**“) – hat einen Code of Business (den „**Kodex**“) eingeführt, der das Engagement von T-Mobile im Bereich ethischer Geschäftspraktiken widerspiegelt.

Alle T-Mobile-Mitarbeiter müssen sich an die in diesem Kodex formulierten Standards halten und jegliche Verstöße gegen T-Mobile-Richtlinien, den Kodex sowie gegen geltende Gesetze und Vorschriften melden. Über die Integrity Line können Mitarbeiter bzw. betroffene Dritte Bedenken äußern oder Handlungsanleitungen dazu erbitten, wie sie sich bei vermuteten Verstößen oder Verdachtsfällen verhalten sollen.

2. Wer ist für die Datenverarbeitung verantwortlich?

SprintLink ist als „Datenschutzbeauftragter“ (Controller) für die Verarbeitung personenbezogener Daten im Rahmen der Integrity Line verantwortlich. Der Datenschutzbeauftragte von SprintLink kann über diese E-Mail-Adresse kontaktiert werden: privacy@t-mobile.com.

3. Welche Informationen können über die Integrity Line gemeldet werden?

Bei einem vermuteten Verstoß gegen den Kodex sollten Sie diesen an Ihren direkten Vorgesetzten oder örtlichen Manager melden. Bei Bedenken gegen eine örtliche Berichterstattung oder wenn Sie nach einer Berichterstattung der Auffassung sind, dass Ihr Bericht nicht angemessen gewürdigt wurde, können Sie Ihre Bedenken in Bezug auf die unten aufgeführten Themen über die Integrity Line an die Muttergesellschaft in den Vereinigten Staaten melden, sofern der Bericht einen Manager (Entscheidungsträger) innerhalb von SprintLink betrifft.

Sie können Angaben zu folgenden tatsächlich stattgefundenen bzw. vermuteten Verstößen machen („**Relevante Angelegenheiten**“):

(1) jede gezielte unethische bzw. fragwürdige Aufzeichnung von Buchhaltungs- und Finanzunterlagen oder Berichten;
(2) das Anbieten bzw. Annehmen von Geschenken oder Zahlungen an bzw. von Anbietern, Lieferanten, Händlern, sonstigen Dritten oder Regierungsbeamten mit der Absicht einer sittenwidrigen Beeinflussung;
(3) jeden Verstoß gegen bzw. jede Nichteinhaltung von Regeln, Vorschriften oder Gesetzen;
(4) wenn die Handlung eines Mitarbeiters oder ein sonstiger Umstand eine Situation erzeugt, in der ein Mitarbeiter seiner Pflicht zur Loyalität gegenüber T-Mobile oder im besten Interesse des Unternehmens zu handeln nicht uneingeschränkt nachkommen kann;
(5) den unbefugten Zugriff auf, die Offenlegung oder den Missbrauch von vertraulichen Kundeninformationen;
(6) die Verweigerung üblicher Privilegien bzw. Rechte aufgrund der Zugehörigkeit zu einem geschützten Personenkreis;

(7) den unbefugten Zugriff auf, die Offenlegung oder den Missbrauch von vertraulichen Mitarbeiterinformationen;
(8) jeden Umstand, in dem gefährliche Materialien oder Abfälle unsachgemäß gelagert, gehandhabt oder entsorgt oder die Nachhaltigkeitsrichtlinien des Unternehmens verletzt werden;
(9) jede vorsätzliche Täuschung zur Erzielung eines unlauteren oder rechtswidrigen Gewinns;
(10) jedes unerwünschte, einschüchternde, feindselige oder missbräuchliche Verhalten aufgrund der Zugehörigkeit zu einem geschützten Personenkreis;
(11) jede Nichteinhaltung von Richtlinien, Gesetzen oder Vorschriften, die sich auf die Gesundheit oder Sicherheit von T-Mobile-Mitarbeitern, Geschäftspartnern, Händlern oder Kunden negativ auswirken;
(12) jegliche gegen eine Person gerichteten Vergeltungsmaßen, weil sich diese Person einer rechtswidrigen Beschäftigungspraxis widersetzt oder eine Anklage erhoben, als Zeuge ausgesagt oder eine Untersuchung unterstützt bzw. daran teilgenommen hat;
(13) jegliche Handlungen oder Umstände, die die Sicherheit von Mitarbeitern, Händlern, Geschäftspartnern oder Kunden beeinträchtigen;
(14) jegliche unerwünschten und beleidigenden sexuellen Annäherungen bzw. sexuell beleidigenden Bemerkungen oder Handlungen;
(15) den unbefugten Zugriff auf, die Offenlegung oder den Missbrauch von vertraulichen oder geschützten Geschäftsinformationen von T-Mobile;
(16) Vorfälle im Zusammenhang mit der Entnahme von Bargeld, Waren oder sonstigem Eigentum ohne Anwendung von Gewalt; und
(17) wenn ein Mitarbeiter durch vorsätzliches Fehlverhalten oder Fahrlässigkeit das Firmeneigentum zerstört, beschädigt oder verschwendet.

Bedenken in Bezug auf oben nicht aufgeführte Angelegenheiten sind an den direkten Vorgesetzten oder örtlichen Manager zu richten und dürfen nicht über die Integrity Line gemeldet werden.

4. Wie erstellt man einen Integrity-Line-Bericht?

Alle Relevanten Angelegenheiten sind über die T-Mobile Integrity Line an https://www.t-mobile.com/responsibility/legal/integrity-line zu melden. Die Integrity Line wird vom konzernfremden Unternehmen Convercent, Inc., 3858 Walnut Street, Suite Nr. 255, Denver, CO 80205, USA („**Convercent**“) verwaltet.

SprintLink empfiehlt Ihnen ausdrücklich, Berichte anonym und ohne Eigenidentifikation zu erstellen. Sie sind nicht verpflichtet, Ihre Identität oder andere Sie betreffende personenbezogene Daten offenzulegen. Anonym eingereichte Berichte haben für Sie keine negativen Folgen. SprintLink wird Mitarbeiter weder disziplinieren, noch diskriminieren oder Vergeltungsmaßnahmen gegen diese ergreifen, wenn sie einen anonymen Bericht in gutem Glauben eingereicht haben. Sich selbst in einem Bericht zu identifizieren ist eher die Ausnahme als die Regel.

5. Welche personenbezogenen Datenkategorien können aufgrund eines Integrity-Line-Berichts verarbeitet werden?

Folgende personenbezogenen Datenkategorien können verarbeitet werden:

- Die Identität, Funktion und Kontaktdaten (z. B. Vor- und Nachname, Anmeldedaten, Identifikationsnummer, Berufsbezeichnung, Arbeitsadresse, Telefonnummer, E-Mail-Adresse) der berichtenden Person. Personenbezogene Daten über die berichtende Person werden nur dann verarbeitet, wenn die berichtende Person ausnahmsweise freiwillig ihre Identität bei der Einreichung des Berichts offenlegt.
- Die Identität, Funktion und Kontaktdaten der Personen, die Gegenstand der

Berichterstattung sind.

- Die Identität, Funktion und Kontaktdaten der Personen, die an der Verarbeitung der gemeldeten Tatsachen beteiligt sind.
- Die personenbezogenen Daten, die in (i) den gemeldeten Fakten, (ii) in den Mitteilungen und sonstigen Informationen, die im Zusammenhang mit der Berichterstattung und der anschließenden Untersuchung der gemeldeten Fakten gesammelt und überprüft wurden und (iii) im Untersuchungsbericht enthalten sind.
- Die personenbezogenen Daten, die in den Informationen zum Ergebnis und den Konsequenzen der Untersuchung zur gemeldeten Faktenlage enthalten sind.

Ihre Angabe Ihrer personenbezogenen Daten als der Person, die einen Bericht gemäß den hier beschriebenen Verfahren erstellt, erfolgt freiwillig. SprintLink kann auf einen von Ihnen eingereichten Bericht eventuell nur mit einer Verzögerung oder überhaupt nicht reagieren, wenn Sie keine personenbezogenen Daten zu den gemeldeten Tatsachen angeben. Die Angabe Ihrer Identität ist in jedem Fall freiwillig und es wird keine negativen Auswirkungen geben, wenn Sie Ihre Identität nicht offenlegen.

6. Welchen Zweck verfolgt die Datenverarbeitung?

Die Verarbeitung der in Integrity-Line-Berichten übermittelten und während einer Untersuchung festgestellten personenbezogenen Daten ist wichtig, um den Kodex umzusetzen, die Einhaltung der geltenden Gesetze durch das Unternehmen sicherzustellen und die Integrität und Ethik der Geschäftspraktiken aufrechtzuerhalten. Sie ermöglicht die Untersuchung der gemeldeten Verhalten und die Umsetzung der Korrekturmaßnahmen, die auf einer in dieser Mitteilung beschriebenen Untersuchung basieren.

7. Auf welchen Rechtsgrundlagen basiert die Datenverarbeitung?

Es gibt folgende Rechtsgrundlagen für die Verarbeitung personenbezogener Daten durch SprintLink im Zusammenhang mit der Integrity Line:

- Die Verarbeitung der Daten ist im Rahmen der berechtigten Interessen, die SprintLink und/oder T-Mobile aufgrund einer Abwägung der berechtigten Interessen von SprintLink und/oder T-Mobile und der berechtigten Interessen bzw. Grundrechte und Grundfreiheiten der betroffenen Personen verfolgen erforderlich.Zu den berechtigten Interessen von SprintLink und/oder T-Mobile gehört die Untersuchung möglicher Verstöße gegen den Kodex und die Ergreifung geeigneter Maßnahmen im Zusammenhang mit den Relevanten Angelegenheiten, um so die Einhaltung des Kodex sicherzustellen und damit zusammenhängende rechtliche Ansprüche zu begründen, auszuüben oder zu verteidigen. Zu den berechtigten Interessen von SprintLink und T-Mobile gehören außerdem:
  - die Verhinderung von Betrug und Fehlverhalten im Zusammenhang mit der Rechnungslegung, den betriebsinternen Kontrollen der Buchführung, den Prüfungsangelegenheiten und der Berichterstattung;
  - die Bekämpfung von Bestechung, der Banken- und Finanzkriminalität sowie von Insidergeschäften; und
  - der Schutz legitimer Umweltinteressen und der Menschenrechte.

  Die Nichtbeachtung dieser berechtigten Interessen kann schwerwiegende Folgen für SprintLink und/oder T-Mobile haben.

- Außerdem sehen die gesetzlichen Regelungen bei einem begründeten Verdacht, dass ein Mitarbeiter während seiner Beschäftigung eine Straftat begangen hat, die Verarbeitung personenbezogener Daten zur Aufdeckung von Straftaten vor, sofern diese Verarbeitung der Daten zur Aufklärung der Straftat erforderlich ist, die berechtigten Interessen des Arbeitnehmers nicht überwiegen und eine Datenverarbeitung nicht unverhältnismäßig ist.

8. Wer kann die Integrity Line nutzen?

Einzelpersonen, einschließlich Mitarbeiter und leitende Angestellte von T-Mobile und seinen Tochtergesellschaften, Vorstandsmitglieder von T-Mobile, Geschäftspartner (einschließlich Vertreter, Auftragnehmer, Verkäufer und Lieferanten) sowie sonstige Dritte können Berichte gemäß dem obigen Abschnitt 3 erstellen.

9. Werden Informationen vertraulich behandelt?

Wenn Sie (ausnahmsweise ohne anonyme Berichterstattung) Ihre Identität bei der Einreichung Ihres Berichts offenlegen, werden Ihre Identitätsdaten wie folgt verarbeitet:

Die Identität einer Person, die einen Bericht in gutem Glauben einreicht, wird nach Möglichkeit vertraulich behandelt. Nur diejenigen Personen werden die Berichte in Empfang nehmen und verarbeiten, die davon unbedingt Kenntnis erlangen müssen. Diese Personen unterliegen einer besonderen Verschwiegenheitspflicht.

Grundsätzlich wird die Identität einer Person, die einen Bericht in gutem Glauben einreicht, nicht gegenüber Dritten offengelegt. SprintLink ist jedoch nach geltendem Datenschutzrecht grundsätzlich dazu verpflichtet, der beschuldigten Person (oder einer anderen im Bericht genannten Person) innerhalb eines Monats nach Berichtseingang Ihre Identität mitzuteilen. Für dieses Prinzip gibt es außerdem folgende Ausnahmen:

- wenn die Weitergabe der Identität der berichtenden Person zur ordnungsgemäßen Verarbeitung und/oder zur Durchführung weiterer Untersuchungen und/oder zur Ergreifung von Maßnahmen im Lichte der Ermittlungen zumutbar ist;

- wenn die Offenlegung der Identität der berichtenden Person gesetzlich verlangt wird (dies kann – unter dem Vorbehalt einer gesetzlichen Verpflichtung unsererseits, einer solchen Aufforderung nachzukommen – eine Aufforderung einer Aufsichtsbehörde sein, die Identität einer berichtenden Person bekanntzugeben).

10. Werden personenbezogene Daten an Dritte und ins Ausland weitergegeben?

T-Mobile US, Inc. und Convercent haben ihren Sitz in den USA. Nach Angaben der Europäischen Kommission bieten die Vereinigten Staaten keinen angemessenen Datenschutz. Mit den folgenden Schutzmaßnahmen soll sichergestellt werden, dass die Übermittlung personenbezogener Daten an T-Mobile US, Inc. und Convercent den Anforderungen von Art. 44 ff. DSGVO entspricht:

- SprintLink und T-Mobile US, Inc. haben einen entsprechenden Datenübertragungsvertrag auf Grundlage der Standardvertragsklauseln (2004/915/EG) geschlossen.
- Convercent verarbeitet über die Integrity Line eingegangene Daten nur gemäß den Anweisungen einer die Standardvertragsklauseln (2010/87/EU) enthaltenden Datenverarbeitungsvereinbarung.

Die in diesem Abschnitt genannten Vereinbarungen können vom Chief Privacy Officer von T-Mobile unter privacy@t-mobile.com angefordert werden.

11. Was passiert mit Ihrem Bericht?

Ausreichend spezifische und sich auf Relevante Angelegenheiten beziehende Berichte werden an die Compliance- und Ethikabteilung von T-Mobile zur weiteren Überprüfung und Untersuchung weitergeleitet.

Je nach Gegenstand der Berichte werden diese – soweit erforderlich – mit Beratern, Forensikern oder Wirtschaftsprüfungsunternehmen geteilt.

Ein Bericht, der sich auf Nicht-Relevante Angelegenheiten bezieht wird abgelehnt und gelöscht und der Berichterstatter wird darüber informiert, dass er die Angelegenheit an die örtlichen Stellen richten soll, da der Bericht nicht über die Integrity Line bearbeitet werden kann.

Stellt sich ein Bericht im Laufe einer Untersuchung als richtig heraus, wird der Vorgesetzte bzw. die Vorgesetzten der betroffenen Mitarbeiter je nach Schweregrad und Inhalt des verifizierten Berichts informiert, sofern dies zur Behebung bzw. Sanktionierung des geprüften Fehlverhaltens erforderlich ist.

Es gibt keine automatisierte Entscheidungsfindung.

12. Mitteilungen an die von einem Bericht betroffenen Mitarbeiter

Die von einem Bericht betroffenen Mitarbeiter werden so bald wie möglich von diesem Umstand informiert, nachdem der Bericht gemäß geltendem Recht registriert wurde. Diese Benachrichtigungen können sich jedoch verzögern, wenn dies aufgrund der Ermittlungen oder zu sonstigen Beweiszwecken erforderlich ist.

13. Welche Folgen hat ein missbräuchlicher Bericht?

Missbräuchliche Berichte, so auch böswillige Berichte, können zu Disziplinarmaßnahmen führen, die selbst die Beendigung des Arbeitsverhältnisses sowie gerichtliche Sanktionen gemäß den geltenden Arbeitsgesetzen und sonstigen geltenden Regeln bzw. Vorschriften umfassen können.

14. Informationshaltung bzw. Vorratsdatenspeicherung

Alle aufgrund eines Berichts gesammelten Daten werden nur so lange wie notwendig aufbewahrt und dies für den Zweck erforderlich ist, für den sie gemäß den geltenden Gesetzen gesammelt wurden (siehe unten).

Personenbezogene Daten im Zusammenhang mit Berichten, die sich als unbegründet herausgestellt haben, werden unverzüglich gelöscht. Personenbezogene Daten im Zusammenhang mit zu Untersuchungen führenden Berichten werden unverzüglich und in der Regel innerhalb von zwei Monaten nach Abschluss der Untersuchungen gelöscht oder anonymisiert. Werden hingegen Disziplinarmaßnahmen oder Gerichtsverfahren eingeleitet, werden die entsprechenden Daten bis zum endgültigen Abschluss dieser Verfahren aufbewahrt.

15. Rechte in Bezug auf personenbezogene Daten

Personen (z.B. berichtende oder von einem Bericht betroffene Personen) haben in Bezug auf die entsprechend dieser Richtlinie verarbeiteten personenbezogenen Daten eine Reihe von Rechten. Diese werden nachfolgend zusammengefasst. Bitte beachten Sie, dass die Ausübung dieser Rechte bestimmte, im geltenden Recht (z. B. der DSGVO) festgelegte Anforderungen bzw. Voraussetzungen erfüllen muss. Diese Rechte können durch lokale Datenschutzgesetze eingeschränkt sein.

Einzelpersonen können bei einer Datenschutzaufsichtsbehörde auch eine Beschwerde einreichen.

Wenn Sie diese Rechte ausüben möchten, wenden Sie sich bitte an privacy@t-mobile.com.

(i) Widerrufsrecht

Hat eine Person, insbesondere die berichtende Person, die Zustimmung zur Verarbeitung personenbezogener Daten erklärt, kann sie diese Zustimmung jederzeit mit zukünftiger Wirkung widerrufen. Der Widerruf einer Einwilligung zur Datenverarbeitung hat keinen Einfluss auf die Rechtmäßigkeit der Datenverarbeitung vor dem Widerruf.

(ii) Auskunftsrecht

Einzelpersonen haben möglicherweise einen Anspruch darauf, von SprintLink eine Bestätigung darüber zu erhalten, ob ihre personenbezogenen Daten verarbeitet werden. Gegebenenfalls können sie auch Auskunft darüber verlangen, in welchen Kategorien und zu welchem Zweck ihre personenbezogenen Daten verarbeitet und an welche Empfänger bzw. Empfängerkategorien ihre personenbezogenen Daten weitergeleitet wurden. Einzelpersonen haben ein Recht auf eine Kopie der verarbeiteten personenbezogenen Daten.

Dies kein absolutes Recht, da möglicherweise auch die Interessen anderer berücksichtigt werden müssen. Die Interessen der anderen Personen können das Auskunftsrecht einschränken. Das Auskunftsrecht gilt beispielsweise dann nicht, wenn eine Auskunft Informationen offenlegen würde, die nach geltendem Recht oder aufgrund ihres Inhalts – insbesondere aufgrund der übergeordneten berechtigten Interessen Dritter – geheim gehalten werden müssen.

(iii) Recht auf Berichtigung

Einzelpersonen können von uns möglicherweise die Berichtigung ungenauer und sie betreffender personenbezogener Daten verlangen. Je nach Verarbeitungszweck haben Einzelpersonen einen Anspruch darauf, unvollständige personenbezogene Daten – auch durch ergänzende Erklärung – vervollständigen zu lassen.

(iv) Recht auf Löschung (Recht auf Vergessenwerden)

Einzelpersonen können einen Anspruch darauf haben, die Löschung der sie betreffenden personenbezogenen Daten zu beantragen.

(v) Recht auf Einschränkung der Verarbeitung

Unter bestimmten Umständen haben Sie möglicherweise einen Anspruch darauf, dass wir die Verarbeitung Ihrer personenbezogenen Daten einschränken. In einem solchen Fall werden die betroffenen Daten gekennzeichnet und dürfen von uns nur für bestimmte Zwecke verarbeitet werden.

(vi) Recht auf Datenübertragbarkeit

Einzelpersonen haben möglicherweise einen Anspruch darauf, von ihnen bereitgestellte und sie betreffende personenbezogene Daten in einem strukturierten, allgemein verwendeten und maschinenlesbaren Format zu erhalten. Sie haben möglicherweise ein zusätzliches Recht, diese Daten an eine andere Stelle zu übermitteln.

(vii) Widerspruchsrecht

Einzelpersonen können unter bestimmten Umständen (aufgrund ihrer besonderen Situation) jederzeit der Verarbeitung ihrer personenbezogenen Daten durch uns widersprechen. Wir dürfen ihre personenbezogenen Daten dann nicht mehr verarbeiten.