[Singapore] Sprint International Communications Singapore Pte Ltd
INTEGRITY LINE DATA PRIVACY POLICY

1. What is the T-Mobile Integrity Line?

T-Mobile US, Inc. with its registered address at 12920 Se 38th St., Bellevue, WA 98006, USA and its subsidiaries (together "**T-Mobile**") including Sprint International Communications Singapore Pte Ltd (UEN 200002645D), a company incorporated in Singapore with registered address at 38 Beach Road #29-11 South Beach Tower Singapore 189767 ("**SprintLink**"), have implemented a Code of Business Conduct ("**Code**") reflecting T-Mobile's commitment to ethical business practices.

All T-Mobile employees are expected to conduct themselves with the standards in the Code and are herewith required to speak up and report any violations of T-Mobile policies, the Code, or any law or regulation. The Integrity Line is one way employees or interested third-parties can raise concerns they may have, or to request guidance on what to do if they think there is a violation or something doesn't seem right.

2. Who is responsible for the processing of the data?

SprintLink is the "controller" responsible for the processing of personal data in conjunction with the Integrity Line. SprintLink's data protection officer can be contacted as follows: privacy@t-mobile.com.

3. Which information may be reported through the Integrity Line?

If you believe a violation of the Code has occurred, you should report such suspected violation to your immediate supervisor or local manager. If you are not comfortable reporting locally, or after reporting, you do not believe your report has been adequately addressed, you may report concerns relating to the topics listed below to the parent company located in the United States via the Integrity line.

You may report concerns about the following actual or suspected violations ("**In Scope Matters**"):

- the purposeful, unethical or questionable recording of accounting and financial records or reports,
- providing or accepting gifts or payments to/from vendors, suppliers, dealers, other third parties or government officials with intent to wrongly influence,
- violations of or failure to comply with a rule, regulation, or law,
- when the action of an employee or other creates a situation in which the employee's duty of loyalty to T-Mobile or ability to act in the company's best interest is compromised,
- unauthorized access to, disclosure, or misuse of a customer's information,
- the denial of normal privileges or rights based on an individual's protected class,
- unauthorized access to, disclosure, or misuse of an employee's information,
- any situation involving the improper storage, handling, or disposal of hazardous or waste material or failure to abide by company sustainability policies,
- deliberate deception to secure unfair or unlawful gain,
- unwelcome, intimidating, hostile, or abusive conduct,
- failure to comply with a policy, law, or regulation negatively impacting the health or safety of T-Mobile employees, business partners, dealers, or customers,
- any form of retribution against an individual because he or she has either opposed an unlawful employment practice or made a charge, testified, assisted or participated in an investigation,
- an action or situation impacting the security of employees, dealers, business partners, or customers,
- any unwanted and offensive sexual advances or sexually offensive remarks or acts,

- unauthorized access to, disclosure, or misuse of T-Mobile confidential or proprietary business information,
- incidents related to the taking of cash, merchandise, or other property without the use of force, and
- when an employee engages in the destruction, loss, or waste of company assets either through willful misconduct or negligence.

Concerns about matters other than those listed above should be directed to your immediate supervisor or local manager and may not be reported through the Integrity Line.

4. How to make an Integrity Line report?

You may report any In-Scope Matters through the T-Mobile Integrity Line at https://www.t-mobile.com/responsibility/legal/integrity-line. The Integrity Line is administered by third-party Convercent, Inc., 3858 Walnut Street, Suite #255 Denver, CO 80205, USA ("**Convercent**").

SprintLink expressly encourages you to provide your report strictly anonymously and without identifying yourself. You are not required to disclose your identity or any other personal data relating to you. Filing a report anonymously will have no negative consequences for you. SprintLink will not discipline, discriminate or retaliate against any employee who files a report anonymously in good faith. Identifying yourself when making a report is the exception rather than the rule.

5. Which categories of personal data may be processed as a result of an Integrity Line report?

The following categories of personal data may be processed:

- identity, function and contact details (e.g., first and last name, verification credentials, job title, work address, phone number, email address) of the reporting person - only if the reporting person has given his/her express consent. Therefore, any personal data about the reporting person is only processed if the reporting person voluntarily chooses, as an exception, to disclose his/her identity when filing the report;
- identity, function and contact details of the persons subject of the reporting,
- identity, function and contact details of the persons involved in the processing of the facts reported;
- personal data contained in (i) the facts reported, (ii) communications and other information collected and reviewed in connection with the reporting and the subsequent investigation of the facts reported, and in (iii) the investigation report; and
- personal data contained in information pertaining to the outcome and consequences of the investigation of the facts reported.

Your provision of personal data as a person making the report in accordance with the procedures outlined herein is voluntary. Failing to provide personal data in relation to the reported facts may delay or make it impossible for SprintLink to act upon any report you submit. The provision of your identity in any case is voluntary and there are no negative effects associated with not providing your identity.

6. What are the purposes of data processing?

The processing of personal data contained in reports submitted via the Integrity Line and obtained throughout any investigation is essential to implement the Code, ensure corporate compliance with applicable law and maintain integrity and ethics in business practices. It enables the investigation of the reported conduct and any necessary corrective measures on the basis of such investigation, as set out in this notice.

7. What are the legal bases for data processing?

The legal bases for Integrity Line-related processing of personal data by SprintLink are:

- The processing is necessary for the legitimate interests pursued by SprintLink and/or T-Mobile based on an assessment SprintLink and/or T-Mobile's legitimate interests and the relevant data subjects' interests or fundamental rights and freedoms. SprintLink's and/or T-Mobile's legitimate interests include investigating and taking appropriate action related to a potential violation of the In Scope Matters Code thereby ensuring compliance and to establish, exercise or defend legal claims in this context. SprintLink's and T-Mobile's legitimate interests also include:
    - prevention of fraud and misconduct in respect of accounting, internal accounting controls, auditing matters and reporting;
    - the fight against bribery, banking and financial crime and insider trading; and
    - the protection of legitimate environmental interests and human rights.

  Failure to pursue these legitimate interests may have severe consequences for SprintLink and/or T-Mobile.

- We may also rely on the statutory justification that allows the processing of personal data to detect crimes if there is documented reason to believe that an employee has committed a crime while employed, and the processing of such data is necessary to investigate the crime, is not outweighed by the employee's legitimate interests, and is not disproportionate.

- With respect to the identity of the reporting person, if the reporting person voluntarily chooses by way of an exception to the anonymous reporting rule to disclose his/her identity when filing the report, SprintLink then relies on the reporting person's consent for the processing of the reporting person's personal data.

8. Who may use the Integrity Line?

Individuals, including employees and officers of T-Mobile and its subsidiaries, the members of the T-Mobile Board of Directors, business partners (including agents, contractors, vendors, and suppliers) and other third parties may make reports in accordance with Section 3 above.

9. Is the information kept confidential?

If you choose (by way of an exception to the rule of anonymous reporting) to disclose your identity when filing your report, your identity data will be treated as described below:

The identity of a person making a good faith report will be processed in a confidential manner wherever possible. Only persons with a strict need to know will collect and process the reports. These persons shall be subject to a specific duty of confidentiality.

In principle the identity of a person making a good faith report will not be disclosed to third parties. There are also the following exceptions to this principle:

- if sharing the person's identity is reasonably necessary for the correct processing of the report and/or to carry out further investigation and/or take measures in light of the investigation;

- if disclosing the person's identity is necessary by law (which may include a request by a regulator to know the identity, provided that we are legally obliged to comply with such a request).

10. Will personal data be transferred to third parties and abroad?

T-Mobile US, Inc. and Convercent are located in the United States. The transfer of personal data outside of Singapore to T-Mobile US, Inc. and Convercent will be protected at a standard that is comparable to that under the Personal Data Protection Act 2012 (No. 26 of 2012) ("**PDPA**"). The following safeguards will be used to ensure that the transfer of personal data to T-Mobile US, Inc. and Convercent are in compliance with the requirements of the PDPA:

- SprintLink and T-Mobile US, Inc. have entered into an appropriate data transfer agreement.
- Convercent processes data received through the Integrity Line only in accordance with instructions under a data processing agreement.

11. What happens to your report?

Reports specific enough and relating to In Scope Matters will be transmitted to T-Mobile's Compliance and Ethics department for further review and investigation as appropriate. To the extent necessary, they will share the report with advisors, forensic or audit firms as appropriate depending on the subject matter of the report.

Out of scope reports will be rejected and deleted and the reporter will be informed that he/she should redirect the concern locally because the report cannot be handled through the Integrity Line.

If a report is verified in the course of the investigation, insofar as required to remedy and/or sanction the verified misconduct, the line manager(s) of the affected employees will be informed, if necessary based on the seriousness and nature of the verified report.

Automated decision making does not take place.

12. Information to employees subject of a report

Employees will be informed as soon as possible of the fact that they have been the subject of a report after the report is recorded in accordance with applicable law. However, such information can be delayed if this is necessary for investigatory or other evidentiary purposes.

13. What are the consequences of an abusive report?

Abusive reports, including reports made in bad faith, may result in disciplinary action, up to and including termination of employment, as well as judicial sanctions in accordance with the applicable employment laws and any other applicable rules or regulations.

14. Information retention

Any information collected as a result of a report will be kept only as long as necessary and for the purpose for which it has been collected in compliance with applicable law, as detailed below.

Personal data relating to reports found to be unsubstantiated shall be deleted without delay. Personal data relating to reports giving rise to an investigation shall be deleted or anonymized promptly and usually within 2 months of completion of the investigation, unless disciplinary measures or legal proceedings are initiated as indicated above, in which case data shall be kept until the final conclusion of such proceedings.

15. Rights with respect to Personal Data

Individuals (such as any reporting person or person subject to a report) have a number of rights in relation to the personal data processed as described in this policy. These are summarised below. Please note that exercising these rights is subject to certain requirements and conditions as set forth in applicable law. These rights might also be limited by local data protection law.

Individuals may wish to lodge a complaint with a data protection supervisory authority.

If you wish to exercise these rights, you should contact privacy@t-mobile.com.

(i) Right of Withdrawal

If individuals, in particular the reporting person, have declared their consent for any personal data processing activities, they can withdraw their consent at any time with future effect. Such a withdrawal will not affect the lawfulness of the processing prior to the consent withdrawal.

(ii) Right of access

Individuals may have the right to obtain from the SprintLink confirmation as to whether their personal data is processed, and if it is, to request access to that personal data including the categories of personal data processed, the purpose of the processing and the recipients or categories of recipients. Individuals have the right to obtain a copy of the personal data undergoing processing.

Because it may be necessary to take into account the interests of others, this is not an absolute right and the interests of other individuals may restrict the right of access. The right of access does, for example, not apply as far as access would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party.

(iii) Right to rectification

Individuals may have the right to obtain from us the rectification of inaccurate personal data concerning them. Depending on the purposes of the processing, individuals may have the right to have incomplete personal data completed, including by means of providing a supplementary statement.