Sprintlink UK 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 SprintLink UK Ltd, 1st Floor, 1 Fore Street, Moorgate, London, EC2Y 9DT, United Kingdom ("**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 in accordance 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 may be compromised;
- unauthorized access to, disclosure, or misuse of a customer's sensitive information;
- the denial of normal privileges or rights based on an individual's protected characteristic(s);
- unauthorized access to, disclosure, or misuse of an employee's sensitive 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;
- unwanted, intimidating, hostile, or abusive conduct that is based on an individual's protected characteristic(s);
- 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 they have 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/or 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;
- when an employee engages in the destruction, loss, or waste of company assets either through willful misconduct or negligence; and
- without prejudice to the above, any other matter which you reasonably believe: (i) is in the public interest; and (ii) tends to show the commission or likely commission of a criminal offence, breach of any legal obligation, a miscarriage of justice, danger to the health and safety of any individual, damage to the environment and/or the deliberate concealing of information about any of the above.

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 a third-party, namely Convercent, Inc. of 3858 Walnut Street, Suite #255 Denver, CO 80205, USA ("**Convercent**").

SprintLink expressly encourages you to provide your identity and contact details when making a report to the Integrity Line. Whilst you are not required to disclose your identity or any other personal data relating to you when reporting, we are more likely to be able to investigate potential wrongdoing promptly, effectively and fairly if you do provide your details. This will also enable SprintLink to liaise with you about steps taken in response to your report, if it is in the position to do so.

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, identification number, job title, work address, phone number, email address) of the reporting persons;
- identity, function and contact details of any persons who are the subject of the reporting, including but not limited to any witnesses and/or the accused;
- 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.

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.

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 of SprintLink and/or T-Mobile's legitimate interests and the relevant data subjects' interests or fundamental rights and freedoms. SprintLink has carried out relevant balancing tests for data processing it carries out on the basis of its legitimate interests; further information on this exercise can be obtained from its data protection officer using the details set out above. SprintLink's and/or T-Mobile's legitimate interests include investigating and taking appropriate action related to the In Scope Matters, including potential violations of the Code, thereby ensuring compliance and to establish, exercise or defend legal claims in this context. SprintLink's and T-Mobile's legitimate interests may 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.

- Where appropriate, we may also rely on the fact that processing is necessary for compliance with a legal obligation to which SprintLink is subject or for the performance of a task carried out in the public interest.

- To the extent that reports made using the Integrity Line require the processing of special categories of personal data (including personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and/or data concerning a person's health, sex life or sexual orientation), SprintLink will also rely on the fact that such processing is necessary for reasons of substantial public interest in accordance with Art. 9(2)(g) GDPR. As appropriate, this may be justified on the basis of preventing or detecting unlawful acts (Data Protection Act 2018, Sch. 1, Part 2, para. 10), regulatory requirements relating to unlawful acts and dishonesty (Data Protection Act 2018, Sch. 1, Part 2, para. 12) and/or the prevention of fraud (Data Protection Act 2018, Sch. 1, Part 2, para. 14).

- To the extent that reports made using the Integrity Line require the processing of personal data relating to criminal convictions and offences, or related security measures, such processing will be carried out, as appropriate, on the basis of preventing or detecting unlawful acts (Data Protection Act 2018, Sch. 1, Part 2, para. 10), regulatory requirements relating to unlawful acts and dishonesty (Data Protection Act 2018, Sch. 1, Part 2, para. 12), the prevention of fraud (Data Protection Act 2018, Sch. 1, Part 2, para. 14) and/or to the extent necessary for the purposes of establishing, exercising or defending legal rights/claims (Data Protection Act 2018, Sch. 1, Part 3, para.33).

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?

To the extent you 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 save as set out below. As part of any investigation, SprintLink will generally be required to disclose your identity to the accused person (or any other person mentioned in the report) Disclosures to other third parties, such as regulators, auditors, forensic service providers, legal advisors and law enforcement may also occur:

- 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; and/or

- 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) or required by law enforcement authorities.

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

In addition to those third parties mentioned above, personal data within any report made via the Integrity Line will be shared with T-Mobile US, Inc. and Convercent, both of which are located in the United States. According to the European Commission, the United States does not provide an adequate level of data protection. 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 Art. 44 et seq. GDPR:

- SprintLink and T-Mobile US, Inc. have entered into an appropriate data transfer agreement based on Standard Contractual Clauses (2004/915/EC).
- Convercent processes data received through the Integrity Line only in accordance with instructions under a data processing agreement that includes the Standard Contractual Clauses (2010/87/EU).

Copies of the agreements referred to in this Section are available by contacting privacy@t-mobile.com.

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 based in the United States 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 they 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 in relation to personal data processed in the context of the Integrity Line.

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 9 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 their personal data processed as described in this policy. These are summarized below. Please note that exercising these rights is subject to certain requirements and conditions as set forth in applicable law (e.g. the GDPR).

These rights may also be limited in certain circumstances, for example if fulfilling a request would reveal personal information about another person, where they would infringe the rights of another (including SprintLink) or if an individual asks us to delete information which we are required by law or have compelling legitimate interests to keep. Relevant exemptions are included in both the GDPR and applicable local laws. SprintLink will inform individuals of any relevant exemptions it relies upon when responding to any request received.

Individuals also have the right to lodge a complaint with a data protection supervisory authority. In the UK, this is the Information Commissioners Office.

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

(i) Right of access

Individuals have the right to obtain from 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.

(ii) 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.

(iii) Right to erasure (right to be forgotten)

Individuals may have the right to request erasure of personal data concerning them.

(iv) Right to restriction of processing

Under certain circumstances, you may have the right to obtain from us restriction of processing your personal data. In this case, the respective data will be marked and may only be processed by us for certain purposes.

(v) Right to data portability

Individuals may have the right to receive personal data concerning them, which they have provided, in a structured, commonly used and machine-readable format and may have the right to transmit that data to another entity.

(vi) Right to object

Individuals may under certain circumstances have the right to object, on grounds relating to their particular situation, at any time to the processing of their personal data by us and we may be required to no longer process their personal data.