Intel Whistleblower Policy & Procedure Guideline Summary

(for Intel Germany)[1]

1. Introduction

Intel is committed to the highest standard of ethics and compliance in our day-to-day business. Our Code of Conduct explicitly states that we stand for "Integrity, Ethical Leadership, Respect, ***Speaking Up*** and Responsibility" and prohibits "Dishonesty, Illegal Activity, ***Retaliation***, Conflicts of Interest, Misuse and Theft of Assets" (emphasis added). These statements are stated on the first page of our Code of Conduct and emphasize that speaking up and non-retaliation are two of our core values that apply to Intel globally, including at Intel Germany GmbH.

Directive (EU) 2019/1937 ("**EU Whistleblower Directive**") was introduced to protect individuals reporting concerns of breaches or misconduct. In response, the German Bundestag passed *Hinweisgeberschutzgesetz*, or the Whistleblower Protection Act" ("**HinSchG**"), which provides legal requirements for covered companies to implement a whistleblower policy and procedure. Intel has a very well-established global whistleblowing and non-retaliation policies and procedures as a "group solution" which satisfies the requirements of the HinSchG.[2] This Intel Whistleblower Policy & Procedure Guideline Summary provides a comprehensive summary of our existing policies and procedures.

2. Speaking Up, Reporting & Investigation Processes

2.1 Speaking Up & Reporting

Internally, all Intel employees are encouraged to speak up and raise concerns when a situation, behaviour, or conduct is or may be inconsistent with our Code of Conduct, company policy or guideline, or applicable law.[3] There are various channels available to report a concern verbally or in writing, including:

i. Managers, general managers, and the Executive Office;
ii. Members of internal Intel groups that specialize in handling reports, including Human Resources, Ethics and Legal Compliance, Internal Audit, Legal,

[1] Intel Germany include i) Intel Germany GmbH & CoKG (LE342); ii) Intel Deutschland GmbH (LE356); iii) Intel Service GmbH (LE346); iv) Intel Magdeburg GmbH (LE365).
[2] "According to the explanatory memorandum to the law, group companies in Germany have the option of accessing a group reporting channel (so-called "group solution"). See, Memo by CMS, May 26, 2023.
[3] Concerns may include not only Intel internal policies but any legal concerns, including concerns relating to criminal law, administrative offences, competition and antitrust laws, public procurement laws, money laundering, environmental laws, human rights laws in federal state or EU regulations.

Employment and Labor Legal ("ELL"), Corporate Security, Information Security, or employee's group or the site Ethics and Integrity Champion;

iii. Intel's Ask Ethics portal;

iv. The Integrity Line, which is hosted by a third party and allows anonymous reporting when permitted by law; and

v. Others procedures established by sites.

While most of the above reporting channels are for internal reporting and are available to Intel employees only, the Integrity Line is externally available for non-Intel employees.

Reports made through the Integrity Line may be made online (Report Online), by calling (Report by Calling) or by mobile application in QR code (QR Code Link). The Integrity Line also supports the German language as a language option.

2.2 Investigation Process

When a concern is raised using any of the channels mentioned above in section 2.1 (including an anonymous report) an objective Intel team will conduct a prompt review of the issue and take appropriate actions based on the findings.[4] Detailed steps are as follows:

i. Appropriate investigation personnel are notified and the case is allocated depending on the issue.[5] At this stage the validity of the concern is determined, a lead investigator is assigned and roles/responsibilities of investigators are defined.

ii. The reporter is notified that his/her reported concern is registered and will be reviewed.[6]

iii. The investigation is conducted, including data collection, research, witness/subject interviews, and notification is made to relevant management/stakeholders.[7]

iv. Following the investigation, evidence is reviewed and the investigators determine the recommendation/remedial action.

v. The findings and recommendation/remedial action are discussed with management/stakeholders.

vi. Recommendation/remedial action is executed and the reporter is notified that the case has been investigated and is closed.[8]

[4] Intel reviews all reported matters seriously, including anonymous reports, even though anonymous reports are not required to be received or processed pursuant to Section 16(1) of the HinSchG.

[5] Intel Investigation team include Legal (Legal & Compliance or HR Legal), HR, Corporate Security, Information Security and Internal Audit.

[6] Throughout the course of investigation, the reporter is kept updated on the investigation where practicable.

[7] All investigations are aimed to be closed within the 60 day period. However, some cases may take longer to complete depending on the complexity.

[8] Details of the outcome may not be shared in detail with the reporter due to confidentiality and data protection reasons.

vii. All evidence and records are kept and maintained centrally online in a strictly confidential manner in compliance with Intel's data privacy and protection policy.

During investigations, all employees are required to make good faith efforts to cooperate fully and provide truthful and complete information whether reports are made internally or externally.

3. Non-Retaliation Policy

Intel has a zero tolerance policy on retaliation against anyone, including externally, who in good faith asks a question, reports a concern about perceived misconduct, or participates in an internal investigation. Retaliation could include any adverse action, such as changing an employee's responsibilities, demoting, transferring, ostracizing, or terminating anyone for raising a question or speaking up in good faith. Any form or shape of retaliation against any reporter, be it internal or external, is treated with utmost severity and is a subject to high priority investigation.

-end-