STMicroelectronics' Misconduct Reporting Hotline
Data Privacy Notice

STMicroelectronics (ST)[1] set up this Misconduct Reporting Hotline service (the Hotline) to provide employees of ST and ST Affiliated Companies[2] as well as interested third parties a channel to report information about potential misconducts when they are unable or do not feel comfortable doing so openly.

This service is operated by GCS Compliance Services Europe Limited[3] (here below referred to as *NAVEX*), an affiliate of NAVEX Global, Inc.[4]. NAVEX is a third party company contracted by ST to set up a communication tool which ensures information exchanged can be handled with the appropriate level of confidentiality while complying with both ST's internal policies and procedures and applicable legal frameworks.

1. Service description

Users of this service (*reporters*) have the possibility to use it to report a ***concern***.

In line with ST's internal procedural framework, the term "***concerns***" collectively refer to concerns, complaints, suspicions and allegations brought to the attention of the Company and regarding possible relevant violation of applicable laws, regulation or of ST Code of Conduct as well as any other internal policies and procedures.

<u>This service is offered by ST as an alternative to open discussion or communication with ST personnel. The use of this service is entirely voluntary.</u>

2. Recipients of ***concerns*** raised through the Misconduct Reporting Hotline

Concerns raised through the Hotline will be reported to the 5 below company executives:

- the Chief Financial Officer (STMicroelectronics International N.V, Swiss branch),
- the Chief Compliance Officer (STMicroelectronics International N.V, Swiss branch),
- the Chief Audit & Risk Executive (STMicroelectronics International N.V, Swiss branch),
- the General Counsel (STMicroelectronics Inc, USA),
- the Corporate VP Human Resources (STMicroelectronics International N.V, Swiss branch).

[1] STMicroelectronics International N.V, Swiss branch

[2] *ST and ST Affiliated Companies* means STMicroelectronics N.V. and any corporation, partnership or any other legal entity, now and thereafter, directly or indirectly controlled by or under common control with STMicroelectronics N.V., provided that such entity shall be considered an Affiliate only for the time during which such control exists. For purposes of this Agreement "Control" shall mean ownership or control, either directly or indirectly, of more than fifty (50) % of the stock or other equity interests entitled to vote for the election of directors or an equivalent governing body.

[3] Registered in the Republic of Ireland, having its principal place of business located in the United Kingdom,

[4] Registered in the United States of America, headquartered in Oregon

Should the ***concern*** raised through the Hotline pertain to misconduct by one of the above listed executives, it will be reported to STMicroelectronics NV's[5] Chief Executive Officer, the Chairperson of the Audit Committee of the Supervisory Board and the Chairperson of the Supervisory Board.

Should the ***concern*** raised through the Hotline pertain to misconduct by the Chief Executive Officer, it will be reported to STMicroelectronics NV's[5] Chairperson of the Supervisory Board, copy to the Chairperson of the Audit Committee of the Supervisory Board.

3. Confidentiality and non-retaliation policy

C*oncerns* raised through the hotline will be treated by ST with the appropriate level of confidentiality (i.e. only shared on a strict need to know basis).

As a general rule, employees or third parties raising ***concerns*** through the Hotline are encouraged to identify themselves in order to facilitate the conduct of the investigation.

However, in countries where anonymous reporting is allowed by the law, reporters can raise ***concerns*** without disclosing their identity.

Should the identity of the reporter be disclosed to ST, it will be protected by the same level of confidentiality as all the information reported through the Hotline. ST will not communicate information that would put a reporter at risk of being retaliated against.

ST has a strict anti-retaliation policy: a reporter should not suffer any adverse consequence for raising a ***concern*** through the Hotline.

All forms of retaliations shall be covered by this strict prohibition, including, but not limited to, adverse consequences on the employee's compensation, benefits, workload, career progression, place of work or working environment.

Corporate Human Resources is responsible for ensuring no retaliation will take place.

4. Communication between ST and reporters

Following the initial report through the Hotline, should the reporter communicate his/her contact details to ST, ST shall use such contact details to communicate directly with the reporter.

Should the reporter of a ***concern*** elect not to disclose his/her identity, the Hotline allows him/her to follow up on a previously raised ***concern***, by providing a report key and a password that can be used to log on back to the platform (similar to a IT hotline "ticket") and see ST's comments or further inquiries posted in response to the ***concern***. This follow up process will be available whether ***concerns*** are reported by phone or via the web.

5. Good faith requirement

Concerns expressed through the Misconduct Reporting Hotline should be made in "good faith" and contain as much specific information as possible to allow for a proper assessment of the nature, extent

[5] STMicroelectronics NV is the holding company of ST, incorporated in the Netherlands

and urgency of the matter that is the subject of the reported ***concern***. "Good faith" does not mean that the reporter has to be right; but it does mean that he/she has firsthand knowledge of the situation reported and believes or reasonably assumes the information provided to be truthful and accurate.

A person who intends to raise a ***concern*** is not expected to gather evidence or to clarify the situation him/herself. But it is important that, at the time the report is sent, the reporter believes that he/she is acting in the best interests of the Company and he/she provides supporting information that can be verified through the conduct of an internal investigation.

Reports intentionally providing false information, designed to harm the Company, disrupt its activities, damage another employee's reputation or to serve the personal interests of their author will not be accepted. Disciplinary action, up to and including termination of employment, may be taken against an employee knowingly raising such malicious ***concerns***.

6. Data privacy statement

The Hotline may capture the following personal data and information provided by the reporter:

(i) the reporter's name and contact details (except for anonymous reports of ***concerns***)
(ii) the reporter's relationship to ST or the ST affiliated company (current or former employee, relative of an employee, employee of a business partner, etc.)
(iii) the name and other personal data of the persons named in the report if such information is provided (i.e.: description of functions and contact details);
(iv) a description of the ***concern*** as well as a description of the circumstances provided by the reporter.

The personal data and information provided by the reporters will be stored in a database which is located on servers hosted and operated in Germany by NAVEX. NAVEX has entered into contractual commitments with ST to secure the information provided by reporters in accordance with applicable law. NAVEX is committed to maintaining stringent privacy and security practices including those related to notice, choice, onward transfer, security, data integrity, access, and enforcement.

For the purpose of processing and investigating reported ***concerns*** and subject to the provisions of local law, the personal data and information provided by reporters may be accessed, processed and used by the relevant personnel of ST or, in limited circumstances, by technical staff at NAVEX or NAVEX Global Inc.. ST's personnel accessing the data may be located in the EU, Switzerland, the United States of America or Singapore.

Adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights for the data transfer to ST´s personal outside the EU is ensured by standard contractual clauses (following EU Model Contracts for the transfer of personal data to third countries) entered into between ST and ST affiliated companies as data controllers.

Technical staff of NAVEX or NAVEX Global Inc. may be located in the United States of America and/or the United Kingdom.

Personal data and information provided by the reporters may also be disclosed by ST to the police and/or other enforcement or regulatory authorities in order to comply with applicable legal obligations.

The relevant bodies that receive and process personal data can be located in the USA or in another country that may not provide the level of data protection available in the EU.

The personal data provided by reporters will be kept as long as necessary to process reports, or, if applicable, as long as necessary to take appropriate action (including but not limited to disciplinary action) or to meet ST's legal or financial reporting obligations. Notwithstanding the foregoing, the personal data will be deleted in accordance with then applicable data protection regulation.

All data collected by NAVEX will be stored on servers located in Germany, with back up in the Netherlands.

Upon ST's request, for the purpose of translating reports, information provided by the reporters in other languages than English may be transferred stored temporarily on a secured platform based in Luxembourg, operated by a subcontractor of NAVEX.

Information presented in one of the official EU language will be accessed by translators based in the EU. Information presented in non-official EU languages maybe accessed to by translators based outside of the European Union in countries that may not provide the level of data protection available in the EU.

In line with the applicable Company procedural framework, ST will notify any Company employee who is the subject of a ***concern*** reported to the Hotline upon completion of the ***concern***'s assessment.

When providing information to the targeted employee(s), ST shall always keep the identity of the reporter confidential and not communicate to the targeted employee(s) information that could allow him/her to identify the reporter.

The subject of the report may access his/her own personal data contained in the report and request correction of such personal data that is inaccurate or incomplete in accordance with applicable law.

Similarly, reporters may also access his/her own personal data contained in the report and request corrections of such personal data in accordance with applicable law.

To make any such corrections, please contact ST's Chief Audit & Risk Executive.

7. Country-specific regulations

Depending on the country in which the reporter is based, the use of the Hotline may be subject to specific regulations such as limitations in the type of issues that can be brought to the Company's attention through the Hotline, the level of seniority of the Company personnel that can be targeted by a ***concern*** or the sensitivity of the information that can be communicated.

ST set up the Hotline's online platform to notify reporters of applicable restrictions based on the selection of the country in which they are based. Should a reporter raise a ***concern*** that would not be compliant with the applicable local regulations, ST will not process such ***concern*** and invite the reporter to raise it through another channel.

All ***concerns***, without any country-specific limitation, can always be openly discussed with ST personnel by phone, email or any other mean of one-to-one communication.