Status: June 2024

Rules of Procedure for the Complaints Procedure under the German Supply Chain Due Diligence Act (LkSG) Information on reporting compliance violations (including ombudsman), data protection and consent to data processing

Siltronic AG and its subsidiaries (together "**Siltronic**") are committed to fighting against all forms of corruption, fraud, other forms of white-collar crime, human rights violations and any form of violation of legal regulations. Employees are therefore required to report (also anonymously) any form of compliance violation to their supervisors or the Compliance Officer. In addition, two further channels for reporting compliance violations are available to Siltronic employees and external parties. On the one hand, the ombudsman appointed by Siltronic AG offers employees and business partners the opportunity to report specific evidence of criminal offences, administrative offences and other legal or regulatory violations anonymously. On the other hand, employees and external parties can report compliance violations as well as information on human rights and environmental risks or breaches of duty in accordance with the German Supply Chain Due Diligence Act (Lieferkettensorgfaltspflichtengesetz) to Siltronic (anonymously) at any time (24/7) via the Integrity Line whistleblower system. The whistleblower system can be accessed from any device (e.g. laptop, cell phone) via a link on the Siltronic website and fulfills all legal requirements for the protection of whistleblowers.

1. Technical protection of the whistleblower system:

The whistleblower system "Integrity Line" is technically managed by the independent operator EQS Group AG (Karlstraße 47, 80333 Munich, Germany, hereinafter "EQS"). The data is stored on external, certified high-security servers operated by Noris Network AG in Germany. The content of the reports is processed exclusively by Siltronic. All data is encrypted, password-protected and stored in a secure location so that access to the content of the data stored electronically in "Integrity Line" is restricted to a narrow circle of authorized persons at Siltronic. EQS cannot view the content of the data stored electronically in the database. As long as you do not provide any personal information, the whistleblower system protects your anonymity by not storing IP addresses, location data, device specifications or other data that could be used to draw conclusions about your identity.

2. No retaliation – no abuse

If you have reported compliance incidents or made a filing to the Complaints Procedure in good faith, neither you nor any person assisting you with the report or any third party associated with you do not have to worry about retaliation or reprisals of any kind. No action will be taken to damage your employment or adversely affect your compensation or career development. Any disciplinary action we impose based on your involvement in the violation will not be considered retaliatory.
Your protection also ends where you are strongly suspected of deliberately making false accusations. Knowingly spreading false or defamatory information is punishable in many countries. You should therefore only disclose information to us or the ombudsman that you believe to the best of your knowledge is accurate. If you knowingly provide us or the ombudsman with false or misleading information, you have to expect negative consequences. Please do not address the public directly. Otherwise, you will deprive Siltronic of the opportunity to clarify a compliance violation internally and to avert a possibly considerable damage from the company. The only exception is if you have reason to believe that there is an immediate or obvious danger to the public interest or a risk of irreversible damage, for example to the physical integrity of a person.

3. What happens after having reported a compliance incident or after a filing to the Complaints Procedure?

Following a report about a compliance incident or a filing to the Complaints Procedure the receipt is documented internally and confirmed to you within seven days. Subsequently the information you provide to us directly or via the ombudsman after your approval will be evaluated and the unit at Siltronic competent for further processing will receive the information you provide. The responsible units include, in particular, the Compliance Officer and the Chief Compliance Officer who assesses whether an in-depth investigation is necessary and in human rights-related cases, the Human Rights Officer. Investigation procedures may be conducted internally or through external investigators (e.g. attorneys, auditors or forensic experts), or may involve government action. If we come to the conclusion that the report or the filing does not require further investigation, we will inform you accordingly within three months. In all other cases, we will initiate a comprehensive clarification of the facts. We will also inform you of this within three months. External specialists that we involve are bound by contractual or statutory confidentiality obligations to maintain the confidentiality of the information you disclose to us. As far as possible and necessary, you will be involved in the clarification of the facts and the development of a solution.

The responsible management within Siltronic will also be informed in order to remedy any shortcomings discovered in the compliance report or the filing to the Complaints Procedure. The audit, legal, and human resources departments are also frequently involved in the processing of compliance reports.

The **purposes** of the collection and processing of personal data in the context of compliance reports or the filings to the Complaints Procedure are

- clarification, termination and sanctioning of serious violations of laws and regulations within and outside the company, as far as they affect the company or its suppliers,
- prevention of such breaches of laws and regulations,
- assertion of claims and rights under civil law, in particular labor law,
- reporting suspected violations of laws and regulations to law enforcement or supervisory authorities.

4. Have government agencies access to my information?

Siltronic may be legally obligated or entitled to disclose information about compliance violations to certain government agencies, including, but not limited to, state investigative agencies or courts. Siltronic may not withhold any information you provide in the event of disclosure, seizure, or confiscation. However, Siltronic will inform you in advance about the release of the information, unless the government agency has explicitly prohibited this.

5. To which countries will my personal data be transferred?

If you have provided personal information in your compliance report or your filing to the Complaints Procedure., we may transfer it to other countries within and/or outside the EU where the confidentiality of personal data is not guaranteed by law to the same extent as in Germany. This applies in particular to countries which, according to EU regulations, are regarded as countries without an adequate level of data protection. Within Siltronic, however, binding internal group policies and agreements ensure an appropriate level of data protection worldwide.

6. Will the person concerned be notified?

Where statutory provisions require that the persons concerned be informed and heard, such persons will be given the opportunity to comment on the information during the investigation. In accordance with the principle of confidentiality, we only name the whistleblower if the disclosure is necessary for follow-up measures and the whistleblower has previously consented to the disclosure in text form.

State authorities may also have corresponding rights to access information or to confiscate information that disclose your name. This may be in particular the case if the person concerned claims that the information provided against him or her is not true, either knowingly or negligently, and files a criminal complaint.

7. How long will personal data be stored?

We will retain your personal data as long as necessary for the clarification and final processing of the compliance report or the filing to the Complaints Procedure., including the elimination of any identified deficiencies and the settlement of any associated legal proceedings. We will also retain your personal data thereafter if this is required or permitted by legal, official or contractual storage obligations. We will delete your personal data as soon as this is legally required, usually three years after the conclusion of the proceedings.

8. Consent and voluntariness.

If you report a compliance violation to us or make a filing to the Complaints Procedure., you consent to the collection, processing and use of your personal data as described above.

If you do not want Siltronic to collect, process, and use your personal information as described, you may also submit your report anonymously to your supervisor or Compliance Officer (e.g., by post, number suppression) or through the whistleblower system or through the ombudsman. The disclosure of your personal data in this process is voluntary. However, we appreciate if you disclose your name to the ombudsman or to us. Many investigations can be carried out more quickly and effectively if the name of the whistleblower is known, since the processor of your report can get in touch with you directly.

9. What rights do I have with regard to my personal data?

Pursuant to the applicable legal provisions, you have the right at any time to **access information** about your stored personal data free of charge, about their origin and the recipient of such data and the purpose of data processing and, if applicable, a right to **correction**, **blocking** or **deletion** as well as to **restriction** of the processing of this data. Please note, however, that we cannot delete or restrict the processing of your data if we need it to fulfil a legal obligation (see Section 6). You can contact us at any time for questions.

You have the right to have data that we process automatically on the basis of your consent or in fulfilment of a contract to be handed over to you or to a third party in a common, machine-readable format. The direct **transfer** of the data to another responsible person will only be carried out as far as it is technically feasible.

10. Contact information

For reports on **compliance incidents** or the filings to the Complaints Procedure.:

- your supervisor
- Compliance-Officer (only for Siltronic employees)
- Ombudsman
- Whistleblower system “Integrity Line”

For reports on **human rights violations**:

We have appointed a human rights officer for our company:

Michael Wirnsberger
michael.wirnsberger@siltronic.com

Tel.: +49 8677 906 86752

- Whistleblower system “Integrity Line”

For the **data processing**:

The **entity responsible** for the data processing is:
Siltronic AG, Einsteinstraße 172, 81677 Munich
Phone: +49 89 8564 3000
e-mail: info@siltronic.com

We have appointed a **data protection officer** for our company.
Tina Klimaschewski
datenschutz@siltronic.com
Phone: +49 8677 90687560

In the event of a breach of data protection law, the person concerned has the right to file a complaint with the competent **supervisory authority**. The responsible supervisory authority for data protection issues is the data protection officer of the federal state in which our company is based. This is

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA),
Promenade 27, 91522 Ansbach