Whistleblower Protection Policy

MAX Automation SE

Status: September 2022

Table of Contents

Preamble

Only if the individuals responsible are aware of the situation can misconduct be corrected and avoided in the future. We therefore ask every employee to point out any misconduct that has been identified.

Besides the Code of Conduct and the Compliance Policy, our compliance reporting procedure is an important component of the Compliance Management System of our Group and its companies.

We provide various reporting channels for internal and external whistleblowers, guarantee their protection against sanctions and thus enable possible misconduct to be reported, comprehensively investigated and clarified.

This Policy describes the procedure for reporting and handling indications of compliance violations. The following issues are addressed in particular:

- What are the reporting requirements?
- What reporting channels exist?
- What responsibilities and procedures apply when dealing with indications of compliance violations?
- What are the principles for taking action in response to identified compliance violations?
- How is the documentation/storage/deletion procedure designed?
- How is feedback to be provided to whistleblowers and how is their protection ensured?

1 Summary

Scope

This Policy applies to MAX Automation SE and to all companies controlled by it ("Group Companies" – together "the MAX Group") and covered by the Whistleblower Protection Act (HinSchG). It fulfills the requirements of the EU Directive 2019/1937 on the protection of whistleblowers ("EU Whistleblower Directive") and its German implementation through the Act for Better Protection of Whistleblowers and for the Implementation of the Directive for the Protection of Persons Reporting Breaches of Union Law ("Whistleblower Protection Act – HinSchG").

Implementation/Target audience

The management of each Group company is responsible for implementing the Policy. All employees in management positions (i.e., persons with budgetary or personnel responsibility) as well as employees who, by virtue of their function, bear special responsibility for ensuring compliance (e.g., employees in the areas of compliance, finance, human resources, legal, auditing, risk management) are required to report.

The whistleblower system is open to all external and internal whistleblowers.

Essential rule content

- Essential compliance violations must be reported to the compliance function (compliance@maxautomation.com). Other reporting obligations remain unaffected.
- A compliance violation is considered essential and reportable if it is likely to cause material damage to a Group company or to MAX Automation SE.
- The reporting officers of the company concerned are responsible for managing the handling of compliance violations and ensuring that all information is followed up on.

- The Group company concerned works closely with the compliance function of the holding company and determines the appropriate measures, e.g. disciplinary measures or process changes, in coordination with the latter in the event that compliance violations are identified.

Contacts

We encourage everyone to report compliance violations through the known and established reporting channels. You may use the electronic whistleblowing system if these reporting channels are not suited for your report. By selecting the Group company concerned, your report will be forwarded to the reporting officer of the respective Group company. Furthermore, you may contact the compliance function of MAX Automation SE (compliance@maxautomation.com).

2 Definitions

Compliance violations

Compliance violations are intentional or negligent infringements (actions and omissions) of statutory provisions (in particular criminal offenses and administrative offenses) or official orders and internal company guidelines (e.g. Code of Conduct or also Group guidelines including this Policy). Violations of contractual obligations (e.g. towards business partners) can also be compliance violations at the same time.

Violations by members of governing bodies (e.g. Board members, Managing Directors), employees or third parties (e.g. business partners such as customers, suppliers, consultants, commercial agents) must be taken into account.

A compliance violation is essential and triggers the reporting obligation pursuant to Section 3 if it is likely to cause material damage to the MAX Group. This is to be assumed if there are objective indications that at least one of the following consequences is to be expected or such a consequence has already occurred:

- The compliance violation constitutes a fraudulent act (e.g. corruption, fraud, embezzlement, theft, misappropriation).
- It is a violation of regulations in the areas of antitrust law or foreign trade law.
- The compliance violation involves the violation of human rights, sexual harassment or a violation of discrimination laws.
- Secrecy regulations are violated in a serious manner.
- The compliance violation causes significant economic damage to a Group company or MAX Automation SE.
- The compliance violation significantly impairs the reputation of a Group company or the MAX Group. This is the case with reporting in regional or national media, for example.
- As a result of the compliance violation, a Group company is threatened with the loss of existing orders or exclusion from future orders (so-called “debarment,” “do-not-source listing,” “black listing,” etc.).
- The compliance violation leads to action by a regulatory or law enforcement authority (e.g., supervisory authority, public prosecutor’s office).
- There are indications of serious breaches of duty involving members of governing bodies or executives (in particular breaches of supervisory duties).
- The compliance violation requires a correction of the accounting.

If there is uncertainty as to whether a compliance violation meets the criteria for a reporting obligation, the compliance function must be consulted.

Reporting points external/internal

Internal reporting offices are the reporting offices established and operated by the MAX Group and its Group companies to which employees of the MAX Group, as well as external parties, can turn.

External reporting offices are the reporting offices of the federal government, of federal authorities as well as of the federal states. The following external reporting offices currently exist:

- Federal Central Reporting Office at the Federal Office of Justice ("BfJ")[1] – https://www.bundesjustizamt.de/EN/Home/Home_node.html
- Reporting Office of the Federal Financial Supervisory Authority ("BaFin") – https://www.bafin.de/EN/Homepage/homepage_node.html
- Bundeskartellamt ("BKartA")[2] reporting office – www.bundeskartellamt.de and in English https://www.bundeskartellamt.de/EN/Home/home_node.html;jsessionid=823E53DC512453AC2DAD30E636B2E739.2_cid390
- Reporting offices of the federal states.

Other terms and definitions

Term	Definition
Information	Information on violations is reasonable suspicion or knowledge of actual or potential compliance violations that have occurred or are very likely to occur, as well as attempts to conceal such compliance violations.
Notifications	Notifications are communications of information about violations to the Notification Center.
Disclosure	Disclosure refers to making information about compliance violations available to the public.
Retaliation	Retaliation is an act or omission related to professional activity that is a response to a report or disclosure and that causes or may cause the whistleblower to suffer an unfair disadvantage.
Follow-up measures	Follow-up actions are those taken by the responsible body within MAX Group to verify the validity of a report, to take further action against the reported violation, or to close the case.

3 Reporting obligations

Essential compliance violations must be recorded by a central office within the MAX Group in order to identify potential compliance risks, verify the adequacy of existing control mechanisms, fulfill legally

[1] https://www.bafin.de/EN/DieBaFin/Hinweisgeberstelle/hinweisgeberstelle_node_en.html;jsessionid=5732D8697625DB96C86A19EBA97D52DB.1_cid501

[2] https://www.bundeskartellamt.de/EN/Banoncartels/Whistle-blower/whistle-blower_node.html;jsessionid=EAD790D2045DC23BB63CEC95724CA5A2.2_cid378

required duties to act, limit potential economic or reputational damage to the MAX Group, and ensure appropriate compliance reporting to the responsible bodies of MAX Automation SE.

If there is a concrete indication or initial suspicion of a material compliance violation, an appropriate local compliance function/reporting office must be informed immediately. The compliance function of MAX Automation SE, which is informed by the reporting officers of the Group companies, is also available as a contact at any time. The reporting obligation applies to indications of committed as well as planned, attempted or incomplete compliance violations.

The following persons are obliged to report:

- All employees in managerial positions (i.e., individuals with budget or personnel responsibility),
- Employees who, by virtue of their function or position on a corporate body, have a special responsibility for ensuring compliance (e.g. employees in the areas of compliance, finance, human resources, legal, auditing, risk management and members of management).

Other reporting obligations within the divisions or legally required reporting obligations remain unaffected.

4 Contact persons

The first point of contact for questions and doubts that employees or managers have about compliance issues should always be their direct supervisors.

- **Direct supervisors**: the first and most important contact person for all employees is the direct supervisor.
- **Compliance function of MAX Automation SE (compliance@maxautomation.com):** is the point of contact for questions or suggestions, as well as for matters subject to reporting in the directive.
- **Local Compliance function / Reporting Office Officer in the company:**

Every Managing Director has appointed Reporting Officers who take the organizational and procedural measures to implement this policy. In cases where there is a serious suspicion that a superior could knowingly be involved in misconduct or is biased, the next higher superior or the management of the Group company must be approached. If involvement or bias must also be assumed in this regard, the Compliance function of MAX Automation SE must be informed.

In addition, it is possible to submit a report – also anonymously – via our electronic whistleblower system. The electronic whistleblower system is available to employees and external persons as a reporting option. If required, the anonymity of the respective whistleblower is always guaranteed within a protected mailbox. Whistleblowers may decide in the system whether they wish to provide their name or remain anonymous. By selecting the Group company, the tips are assigned to the respective Reporting Officers of the Group company. By selecting MAX Automation SE, the information is forwarded to the Central Compliance function of the Group.

The Reporting Officers are independent in the performance of their duties. It is to be ensured that their tasks and duties do not lead to conflicts of interest.

5 Procedure in the event of compliance violations

The compliance function of MAX Automation SE manages and coordinates the handling of compliance violations at the Group level and is to be informed by the Reporting Officers of the Group companies upon receipt of a report. It also advises the Group companies' Compliance Officers as to which body should be tasked with further investigating a report (investigating body). The investigating body is responsible for looking into the content of the compliance information received.

The Reporting Officers of the Group companies must ensure that all indications of such violations are appropriately investigated and

- confirm receipt of a report to the person providing the information within seven days at the latest
- check whether the reported violation is relevant
- keep contact with the person providing the information
- check the validity of the message received
- request further information from the person providing the tip-off, if necessary, and
- take appropriate follow-up measures in coordination with the Compliance function of the holding company

Within three months after acknowledgement of receipt of the report or, if receipt has not been acknowledged, no later than three months and seven days after receipt of the report, the reporting office must provide feedback to the person making the report. This feedback should include notification of follow-up actions planned and already taken and the reasons for these.

Feedback may only be provided to the person providing the information, however, if this does not affect internal inquiries or investigations and does not affect the rights of the data subjects who are the subject of a report or who are named in the report.

6 Electronic whistleblowing system

In our electronic whistleblower system, reports on violations in certain areas can be submitted and inquiries made.

Sequence of the electronic reporting process

The electronic reporting process goes through four stations:

First: The person providing the information receives information about the technical precautions taken to ensure their data security.

Second: The Group company and the subject focus of the report are queried.

Third: The person providing the information is given the opportunity to formulate the message in a free text. Approximately one DIN A4 page of an established word processing program is available for the free text. It is also possible to send one or more files or record a voice message. After the message has been sent, a case ID will be issued as proof that the person providing the information has submitted the message.

Fourth: A protected electronic mailbox can then be set up. This mailbox can then be used for further communication, e.g. feedback, questions etc. If the mailbox is set up for a message, the person providing the information can access this mailbox via an existing interface in the system with a “login.”

At the latest within three months after the notification, a statement is made to the person providing the information. If necessary, shorter deadlines might have to be observed in certain countries.

Ensuring the anonymity of the person providing the information

The protected mailbox requires the person providing the information to select a password. The transmission of the message is secured by encryption and special security routines. When setting up the mailbox, a note is to be made that no data should be entered that would allow conclusions to be drawn about the person providing the information if they choose to remain anonymous.

The technical guarantee of data security is certified and the certificate can also be issued upon request. The procedure chosen complies with EU Directive 2019/1937 on the protection of whistleblowers (“EU Whistleblowing Directive”), which came into force on December 16, 2019.

7 Protection of whistleblowers / prohibition of retaliation

Protection of whistleblowers

Whistleblowers who draw attention to misconduct to the best of their knowledge and beliefs will not suffer any disadvantage as a result. Even participants in possible misconduct benefit from far-reaching amnesties under labor, civil and criminal law, insofar as this is legally permissible and their tip helps to uncover previously unknown misconduct and thereby helps to mitigate the damage to the MAX Group or its companies and prevent it for the future.

This protection includes persons who have made a report or disclosure if, at the time of the report or disclosure, the person making the report had reasonable grounds to believe that the information he or she reported or disclosed was true and the report concerned compliance violations, as defined above, or the person making the report had reasonable grounds to believe what he or she believed at the time of the report or disclosure.

Provided that these requirements are met, the protection also applies to natural persons who confidentially assist the whistleblower in making a report or disclosure in a professional context.

Protection of disclosing persons

Persons who disclose information concerning violations are only protected by the EU Whistleblower Directive and the German Whistleblower Protection Act under the very narrow conditions of this Directive. If serious and irreparable damage to the MAX Group or its companies is likely as a result of the disclosure, it must always be checked in each individual case whether the person making the disclosure has obtained qualified advice in advance.

Ban on retaliation

We ensure that any form of retaliation against whistleblowers is avoided. This is prohibited and also applies to threats and attempts of retaliation. All employees are obligated to refrain from retaliation. Retaliation against whistleblowers constitutes misconduct within the meaning of this policy.

Internal investigations, in particular personal investigations, can only be initiated by the respective company management and in the event of a concrete initial suspicion of a criminal offense or serious breach of duty under labor law.

8 Protection of affected persons

Persons affected by the information are to be informed about the measures taken, insofar as it can be ruled out that the purpose of the investigation will be impeded or that peaceful operations within the company will be disturbed to a disproportionate extent. At the latest when the investigative measures are expressly noted to have ended by the MAX Group or the respective Group company, the affected persons are to be informed of the conclusion of the measures and be heard. We ensure that those affected by reports are treated fairly.

Intentionally communicating misinformation about misconduct by other employees is a violation of this policy at any level of the company and will be considered misconduct.

9 Documentation and data

Data processing and collection

We ensure that unauthorized persons – even if they work for the MAX Group – do not have access to documents (such as e-mail histories) that could allow conclusions to be drawn about the identity of the person making the report. We ensure that the identity of the whistleblower is only known to the persons responsible for receiving reports or taking follow-up action, as well as to the persons assisting them in the performance of these tasks.

The Reporting Office and the authorized bodies within the MAX Group process the personal data contained in the reports. They receive and evaluate them. New personal data is to be collected and further processed for follow-up measures.

The hotlines observe the applicable provisions of the GDPR and the BDSG in the data processing and collection process.

Documentation / Storage / Deletion

The reporting offices responsible for receiving reports document all incoming reports in a permanently retrievable manner in compliance with the applicable provisions of the GDPR and the BDSG and ensuring the protection of the person providing the report.

In the case of telephone messages or messages by means of another form of voice transmission, a permanently retrievable audio recording of the conversation or its complete and accurate transcript (verbatim record) may only be made with the consent of the person providing the information.

In the event that a complete and accurate record of the meeting is made and maintained with the consent of the person providing the information, the person providing the information is to be given the opportunity to review the record, correct it if necessary, and acknowledge it by his or her signature or in electronic form.

The aforementioned documentation will be deleted two years after the conclusion of the procedure.

10 Follow-up measures in the event of compliance violations

Responsibility of the Group company / coordination with the Compliance function

Follow-up measures in response to an identified compliance violation are the responsibility of the Group company concerned. The Group company concerned is responsible for ensuring that the measures comply with all legal requirements.

The responsible management of the business unit or the Managing Director of the Group company concerned shall coordinate the necessary measures with the Compliance function in the event of significant compliance violations for which there is a reporting obligation (see section 3). Legally prescribed duties to act remain unaffected. If advance coordination is not possible due to statutory deadlines for action, this information is to be provided immediately afterwards.

In the event of differences of opinion regarding the appropriateness of the follow-up measures intended by the Group company concerned, the Compliance function shall inform the responsible management of the business unit of this. If no agreement can be reached on the necessary follow-up measures at this level either, the Managing Directors of MAX Automation SE will decide.

Disciplinary follow-up measures for compliance violations

If a compliance violation is identified, the necessity of disciplinary action against responsible employees or managers must be examined. The individual case is to be reviewed. A uniform standard and the principles of fair procedure apply. The rights of the persons concerned are to be protected and confidentiality and data protection are to be ensured.