



B2 - Data Protection, Anti-Bribery and Information Security Policy



A member of

Excellence United

Index

1	PREFACE	3
1.1	Data Protection, Anti-Bribery and Information Security	3
2	DATA PROTECTION, ANTI-BRIBERY AND INFORMATION SECURITY POLICY	3
2.1	Data Protection Policy.....	3
2.1.1	Strategic Goals for Data Protection	5
2.2	Anti-Bribery Policy	5
2.2.1	Strategic Goals for the Anti-Bribery Policy	6
2.3	Information Security Policy	7
2.3.1	Strategic Goals for Information Security	8
3	SUPPORTING DOCUMENTS.....	8

List of figures

None

List of tables

None

1 Preface

Our company develops, produces and installs highly complex production and packaging systems of the highest quality. The systems are used in innovative industrial sectors, particularly the pharmaceutical, medical technology and consumer areas. Our product offerings are supplemented by extensive services concerning the customer product. As a technology leader in various market segments, we are able to offer our customers individualised solutions, from laboratory applications to the production line. Thanks to our global network of branches and representatives, we are always close to our customers.

1.1 Data Protection, Anti-Bribery and Information Security

All employees are responsible for data protection, for combating bribery and for ensuring information security within the scope of their tasks. Compliance with the law is also ensured when performing these tasks.

All employees are therefore required to apply the principles and procedures described in the data protection, anti-bribery and information security instructions. In this way, each individual employee contributes to ensuring our standards.

Compliance is supported and reinforced by the company's Code of Conduct.

2 Data Protection, Anti-Bribery and Information Security Policy

The respective policies and accompanying strategic goals have been defined by the senior management. The policies specify the framework for the implementation of our shared goals. At least once per year, the policies are checked for currentness and usefulness and adjusted if need be.

2.1 Data Protection Policy

➤ Purpose of the Data Protection Policy

- We hereby set the goal to enforce the valid General Data Protection Regulation (GDPR) in our company in order to guarantee privacy and the protection of personal data.

➤ Definitions of Key Terms

- Our use of key terms in connection with data protection is limited to the use of the glossary from the GDPR.

➤ **Principles and Purposes of Data Processing**

- Processing of personal data is always limited to the legitimate aim. In this context, this means absolute data minimisation.
- Personal data is always processed with appropriate security and protection against unauthorised or unlawful processing and at the latest state of the art.
- Personal data is fairly processed with openness and transparency with respect to the data subject and only saved as necessary.
- Corresponding accountabilities are ensured to the full extent.

➤ **Key requirements or controls**

- For the implementation and constant control of data protection according to the GDPR, regular internal audits on the topic are to be performed after a data protection risk analysis.
- These audits should relate to organisational control, methods of access control, data transfer, input and disclosure, order control, availability control as well as the requirement to separate personal data.

➤ **Key Roles and Their Responsibilities**

- HH Internal Data Protection Coordinator
Stefan Mayer
stefan.mayer@hoefliger.de
+49 7191 501 1835
- External Data Protection Officer
(*Contact details withheld*)

➤ **Responsible supervisory authority**

- Officer for Data Protection and Freedom of Information, State of Baden-Württemberg
Dr. Stefan Brink
poststelle@fdi.bwl.de
+49 711 61 55 41 0

2.1.1 Strategic Goals for Data Protection

- We guarantee the highest possible protection of all sensitive and personal data of our employees, customers and partners.
- We ensure that all employees have a high level of awareness in the area of data protection and make continuous improvements in this regard.
- We promote the active cooperation of all employees and thus bolster our defence against data protection risks.

2.2 Anti-Bribery Policy

➤ Purpose of the Anti-Bribery Policy

- Our actions are guided by the specifications of the "Code of Ethics" of the International Society of Automation (ISA) and by ISO 37001, which supports companies in combating bribery.

➤ Our Responsibility

- We always abide by laws and regulations and support internationally recognised human rights.
- We ensure that the interests of individuals do not come into conflict with the interests of the company.

➤ General Principles of Implementation

- Zero tolerance for bribery applies to all employees as well as cooperation partners and business partners, independently of their location and function.
- The entire managing staff are obligated to accept a key role in creating the organisational culture in which bribery will not stand a chance and will not be accepted in any form.
- The anti-bribery policy must be widely communicated and promoted among the employees of the company with the aid of, among other things, training initiatives to facilitate understanding and to apply the rules of the policy in daily life at the company.
- Our conduct is just, honest and friendly; moreover, we strive for openness and transparency in our actions. Thanks to this attitude, we are regarded as a responsible company that can be trusted.

➤ **Currentness and Improvement**

- We ensure our operation into the future through the review, at least once per year, of the currentness and effectiveness of our Anti-Bribery Management System (AKMS).
- Regular training courses, internal and external audits also ensure the high functionality of our Anti-Bribery Management System.

➤ **Procedure in Case of Deviations**

- Deviations are extensively analysed using our centralised Process Action System (PAS) in order to achieve continuous improvement through suitable measures.

2.2.1 Strategic Goals for the Anti-Bribery Policy

- The goal of the policy is to introduce the conditions of zero tolerance for bribery and corruption and measures ensuring compliance with the applicable regulations. These conditions are valid both for employees and for cooperation/business partners.
- Prevention and avoidance of bribery cases and other forms of corruption and immediate reporting after their detection throughout the company.
- Guarantee of the legal requirements in the anti-bribery area.
- Verifiable compliance with the continuous improvement of the bribery prevention process.

2.3 Information Security Policy

➤ Purpose of the Information Security Policy

- We hereby set the goal of introducing and certifying an information security management system in accordance with DIN EN ISO/IEC 27001.

➤ Our Responsibility

- We deliver safe products at a high level of quality following economical production processes.
- All non-public information is protected here against unauthorised access through suitable authorisation measures.

➤ Data Integrity

- Information is always provided in a complete and unmodified form.
- The sending and receiving of information is binding.
- Access to information and the non-public area of the organisation is granted after sufficient authentication.

➤ Data Availability

- Operation of our information technology systems (IT) assures the necessary access to information and functions of all requesting parties with sufficient authorisation.

➤ Currentness and Improvement

- We ensure our operation into the future through the review, at least once per year, of the currentness and effectiveness of our ISMS.
- Regular internal and external audits also ensure the high functionality of our ISMS.

➤ **Procedure in Case of Deviations**

- Deviations are analysed extensively in order to achieve the continuous improvement of our ISMS through suitable measures and ensure the current state of the IT security technology.

2.3.1 Strategic Goals for Information Security

- User-related alignment of our IT systems for effective compliance with legal standards.
- Guarantee of legal requirements and equal protection of personal rights of data subjects (customers, employees, suppliers, etc.)
- Protection of business processes and associated data.
- Verifiable fulfilment of the duty to exercise proper care and prevention of organisational faults.

3 Supporting Documents

- Code of Conduct
- Base Code of the Ethical Trading Initiative