Policy

0011

Binding Corporate Rules (BCR) - Corporate Data Protection

Valid from
2025-05-05

Contents

1. Motivation and objectives

The members of the Festo Group in accordance with Attachment 1.2 "CA 0741 Members of the Festo Group" (hereinafter referred to as the Festo Group) have undertaken to protect personal data and personal rights. The Festo Group's Group-wide Policy "Corporate Data Protection" (Binding Corporate Rules) is a Group-internal regulation for the fulfillment of Data privacy requirements and the creation of a uniform level of Data privacy throughout the Group.

The Festo Group has opted for a Group-wide binding corporate guideline that guarantees mutual recognition of this decision for the member states of the agreement through a special approval and coordination procedure of the supervisory authorities (mutual recognition).

A "group contract on the processing of personal data" is also used for intra-group controller processor agreement under Article 28 GDPR and joint controller agreement under Article 26 (1) 1 GDPR.

This Policy is legally binding for all members of the Festo Group by resolution of the Management Board of Festo SE & Co. KG and contains a clear duty for each Group member, including their employees, to respect this Policy. The management of the Festo Group shall take the necessary Data privacy management measures to ensure compliance with the Policy.

The purpose of this Policy is to ensure adequate protection of personal data that is transmitted and processed within the Festo Group. In addition to the EU data protection regulations (in particular the General Data Protection Regulation, GDPR), the respective national data protection regulations also apply, to which reference is made.

The BCRs are an instrument prescribed and regulated by the EU for the intra-group transfer of personal data. The EU template describes mandatory elements that must be implemented in internal regulations in accordance with the text.

2. Assignment

The Management Board of the Festo SE & Co. KG has assigned this Policy in order to achieve the aforementioned objectives and thus meet the legal requirements and, in particular, Festo's own requirements for the protection of the right to informational self-determination of each individual.

3. Material scope

3.1 Data transfers

This Policy contains data protection regulations to assure personal data in terms of the GDPR, in particular when they are transferred from the European Union (EU) or the European Economic Area (EEA) to third countries whose level of Data privacy is considered inadequate. However, the intra-group regulations also apply worldwide to all other personal data processed by the members of the Festo Group if they originate from the EU or the EEA or are part of the central services of the Festo Group in accordance with Attachment 1.3 "CA 0742 Central Services of the Festo Group". Only for personal data that does not originate from the EU or the EEA and is not part of the Festo Group's central services the intra-group regulations are not applicable. A detailed description of the data flows and transmission processes covered by this Policy can be found in Attachment 1.1 "CA 0740 - Data flows and transmissions".

3.2 Categories of personal data

This Policy applies to personal data processed both, automatically and manually. The Festo Group largely processes the following personal data and data categories for the stated purposes:

- Contact persons of customers, prospects and potential customers: Business contact details including telephone, fax and e-mail details; information about telephone calls; on-site visits and their activities on our websites
- Applicants: Mainly application details; job history details; training and qualification details

- Employees, trainees, placement students, retirees, past employees and dependents: Contractual, master and accounting data; private and business address details; field of activity; salary payments; name and age of relatives if relevant for social welfare benefits; wage tax details; bank details; assets entrusted to the employee; data for personnel management and control; timekeeping data and access control data; schedule management data; data for communication and for processing and monitoring transactions and technical systems; emergency contact data for persons nominated by the employee who should be contacted in an emergency; special categories of data; travel booking and accounting data; image files
- Sales agents / agencies: Address and business details; contract data; contact details
- Contact persons of suppliers / service providers: Address details; contact information; schedule management data; accounting and performance data

4.Addressees of the Policy

This Policy is addressed to employees and managers within the Festo Group.

5.Transparency

The Festo Group commits to provide the data subjects with easy access to this Policy.

- The data subjects can be informed about the transfer and processing of their personal data by one or more of the following measures: Publication on the Group-wide intranet platform "WeNet", on which all binding Policies of the Festo Group are stored
- This Policy is published on the Internet
- Personalized letters, circulars, notices, leaflets or other print media
- Face-to-face meetings, works meetings or other information events
- Announcement of works agreements, contractual arrangements, work instructions or other guidelines Announcement by means of e-mail, on the Internet or portal-based platforms or through the use of other electronic media

6.Definitions of terms

For the purposes of this Policy, the following definitions of terms are used in accordance with the applicable data protection regulations, in particular Art. 4 GDPR:

- **Data subject**: is an identified or identifiable natural person whose personal data is collected, processed or used;
- **Personal data**: is any information relating to a data subject; an identifiable natural person is someone who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **Special categories of personal data**: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;
    - **Genetic data** means personal data relating to the inherited or acquired genetic characteristics of a **natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;**
    - **Biometric data** means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data;
    - **Data concerning health** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
- **Processing**: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

- **Restriction of processing**: the marking of stored personal data with the aim of limiting their processing in the future;
- **Consent of the data subject**: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- **Controller**: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **Processor**: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **Sub-processor:** is any processor engaged by the data importer or by any other processor or sub-processor who agrees to process the received personal data exclusively for the purpose of transfer or in accordance with the instructions of the data exporter or controller, this Policy and the terms of the written contract for sub-processing;
- **Third party**: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;
- **Recipient**: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- **Company**: a natural and legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;
- **Group of companies**: a controlling company and its controlled companies;
- **Data exporter** is the controller or processor in the EU/EEA who transfers personal data to a third country (country outside the EU and EEA);
- **Data importer**: is the controller or processor in a third country who has received data from a data exporter;
- **Data export / import** describes the classic data transfer between IT systems. Data from an IT system of the data exporter is exported by the data exporter to a file that is transmitted to the data importer and imported by the latter into an IT system under its own responsibility. This export/import can be found in many definitions of the BCR template, but is no longer "state of the art", at least at Festo.
- **Data transfer:** In addition to the classic export/import, this also includes targeted or possible access to data. During access, the data is temporarily transferred, processed and then stored again in the source system. Access to data is controlled by personal role concepts, which can be adjusted by the controller if the collaboration is interrupted or terminated. The processor is prohibited from storing the data in a third country.
- **Applicable law** is in each case national/local law of a third country as applicable to a BCR member in these country. In any case, BCR members must comply with the requirements of this BCR.
- **Personal data breach**: a breach of security leading to the accidental or unlawful destruction, , loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- **Technical and organizational measures** refers to those measures aimed at protecting personal data against accidental or unlawful destruction or accidental lass, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing;

- **Competent supervisory authority** means the EEA supervisory authority (Art. 51 GDPR) competent for the data exporter;
- **Binding corporate rules**: personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of companies;
- **File system**: any structured collection of personal data that is accessible according to specific criteria, regardless of whether this collection is managed centrally, decentrally or according to functional or geographical aspects;

- **Profiling**: any form of automated processing of personal data consisting in the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;
- **Pseudonymization**: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

The definitions of terms contained in the GDPR and the applicable national Data protection regulations also apply. The members of the Festo Group commit to interpreting this Policy within the meaning of these regulations.

6.1 Abbreviations

Term / Abbreviation	Term / Explanation
BCR	Policy 0011 Binding Corporate Rules (BCR) - Group data protection According to Art. 47 GDPR
DSMS	Data privacy management system
GDPR	European General Data Protection Regulation
EU	European Union
EEA	The European Economic Area is an enhanced free trade area between the European Union and the European Free Trade Association.
Festo Group	Members of the Festo Group in accordance with Attachment 1.2 " CA 0741 Members of the Festo Group"

7. Purpose limitation

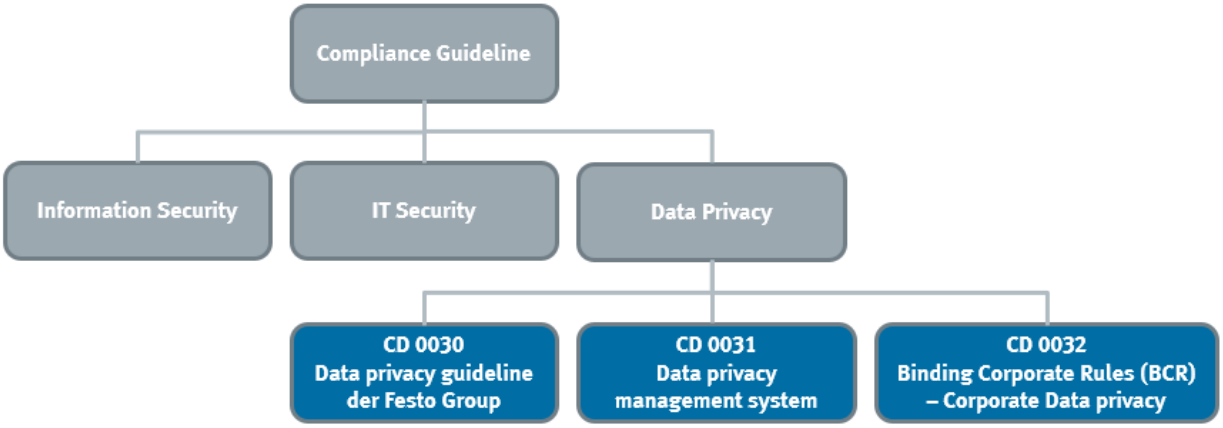
Personal data may only be collected, processed or used in the Festo Group for the purpose indicated prior to processing of the data, or for other purposes evident from the circumstances or provided for by law (purpose limitation requirement).

The Festo Group processes personal data for business purposes. In particular these include

- Production and sales of components and solutions for automation technology and technical education and all associated secondary business activities and actions required to achieve the purpose of the company
- and extending to IT-based activities including the operation of IT systems
- Secondary purposes are accompanying or supporting functions, in particular management of personnel, applicants, customers, suppliers and service providers
- Video surveillance of the company is carried out to protect legitimate interests for the purpose of risk defense, e.g. to prevent damage caused by vandalism, to protect against break-ins and property crimes, to prevent criminal acts and to collect evidence. A risk assessment and, if necessary, a Data protection impact assessment is carried out.

Processing of personal data for own purposes as well as on behalf of the members of the Festo Group
The purpose of the processing and transfer of personal data must be clearly defined and lawful. Personal data must not be processed other than for the indicated purpose.

8. Regulatory environment



9. Basic requirements

9.1 Data privacy principles

The processing of personal data within the Festo Group follows the principles laid down in Data protection law, in particular in Art. 5 GDPR.

Personal data shall be

- processed lawfully, fairly and in a manner in relation to the data subject ("lawfulness, fairness and transparency");
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization");
- processed for no longer or to an extent greater than is necessary for the purposes for which they are collected; storage periods must be limited ("data avoidance and data minimization")
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures ("integrity and confidentiality");

9.1.1. Accountability

The controller is responsible for, and be able to demonstrate compliance with the Data privacy principles. This includes in particular the implementation of the documentation obligations in a records of processing activities in accordance with Art. 30 GDPR.
That record contains the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data privacy officer;
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;

- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;
- where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) GDPR, the documentation of suitable safeguards;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organizational security measures referred to in Article 32(1) GDPR.

9.1.2 Preventive prohibition with reservation of authorization

Personal data may only be collected, processed and used insofar as permitted by EU / EEA data protection laws or other EU / EEA legislation or with the consent of the data subject. In accordance with this "preventive prohibition with reservation of authorization" facts establishing authorization are always required for processing of personal data.

9.1.3 Consent

The data subject's consent must be obtained if there is no legal authorization according to Art. 6 (1) (b) to (f) GDPR for the processing of personal data. This consent is only valid if it was freely given, and the data subject was duly informed in advance about the consequences and scope of the consent (free and informed consent). Consent must be obtained in writing, electronically or in accordance with the relevant Data protection regulations and can be withdrawn at any time by the data subject with effect for the future. The withdrawal option cannot be waived.

9.1.4 Proportionality

Processing is only permissible in accordance with the specifications of the Policy if the processing measures are deemed suitable, necessary and proportionate to achieve the defined purposes based on the legal requirements and a balancing of interests in accordance with the principle of proportionality. All the interests at stake and statutory provisions involved must be included in this overall consideration of the relevant issues.

9.1.5 Immediacy

Personal data should only ever be collected directly from the data subject. Exceptions require special legitimation, especially exceptions due to a legal provision or because collecting the data from the data subject would involve a disproportionate effort and there is no evidence that legitimate specific interests of the data subject will be compromised.

9.1.6 Notification obligation

In accordance with the provisions of Art. 33 and 34 GDPR, data breaches must be notified immediately to the controller, the responsible Data privacy officer or the Data privacy organization. In the case of a personal data breach, the controller shall, through the Data Privacy Officer, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of a natural persons. In this case, where the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, in accordance with the requirements of Art. 34 GDPR, the data subject must be notified without undue delay. Every data breach, including those that are not notified to the competent supervisory authority, must be documented (with the facts relating to the personal data

breach, its effects and the corrective measures taken) and the documentation must be made available to the competent supervisory authority on request.

9.2 Legal basis for processing of personal data

At least one of the following criteria must always be satisfied for processing of personal data by the Festo Group:

- the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes, Art. 6 para. 1 lit. a GDPR serves as the legal basis;
- processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, Art. 6 (1) (b) GDPR serves as the legal basis;
- processing is necessary for compliance with a **legal obligation** to which the controller is subject; Art. 6 para. 1 lit. c GDPR serves as the legal basis;
- processing is necessary in order to protect **the vital interests** of the data subject or of another natural person, Art. 6 para. 1 lit. d GDPR serves as the legal basis;
- processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller or the third party to whom the data are disclosed, Article 6(1)(e) GDPR serves as the legal basis;
- processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child, Art. 6 (1) (f) GDPR serves as the legal basis. Typical cases for the existence of a legitimate interest are especially
    - greater efficiency, security and professionalism, e.g. the assurance of service levels;
    - savings in operating costs, costs of investment in hardware and software licenses and the necessary personnel, e.g. due to a reduced administrative workload;
    - Server location in Germany or Europe;
    - Certification of the service providers;
    - Ensuring information security and preventing cyber attacks, hacking, phishing, etc.;

The processing of personal data relating to criminal convictions and offences is prohibited, unless the same exemptions as the ones envisaged by Art. 10 GDPR apply.

9.3 Special categories of personal data

Special categories of personal data may only be processed in the following cases:

- The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where the applicable laws prohibit this.
- Processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or the data subject in the field of employment and **social security** and social protection **law** in so far as it is authorized by law or a collective agreement providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
- Processing is necessary to protect **the vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a **foundation, association or any other** not-for-profit **body with a** political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

- Processing relates to personal data which are manifestly **made public** by the data subject;
- Processing is necessary for the establishment, exercise or defense of **legal claims** or whenever courts are acting in their judicial capacity.
- Processing is necessary for the purposes of **preventive** or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of legal provisions or on the basis of a contract with a health professional (or professionals or other persons subject to professional secrecy or a duty of confidentiality by virtue of legal provisions or the regulations of national competent authorities).

9.4 Rights of the data subject

- Data subjects have the following rights upon request: **Transparent information**: in accordance with Art. 12 et seq. GDPR to obtain all information regulated by law , see in detail in clause 5 and clause 9.4.1 of this Policy, especially with regard to
  - The legal basis for data processing, purpose limitation and proportionality
  - Data quality, security and confidentiality
  - Transparency and easy access to this Policy BCR
- **Right of access**: to obtain information about the processed personal data in accordance with Art. 15 GDPR, see in detail under clause 9.4.1 of this Policy.
- **Right to rectification**: in accordance with Art. 16 GDPR, to receive without undue delay the rectification of inaccurate or to have incomplete personal data concerning him or her completed, see in detail under clause 9.4.2 of this Policy.
- **Right to erasure**: to obtain the erasure of personal data concerning him or her without undue delay in accordance with Art. 17 GDPR, see in detail under clause 9.4.2 of this Policy.
- **Right to restriction of processing**: to obtain restriction of the processing of personal data in accordance with Art. 18 GDPR, see in detail under clause 9.4.2 of this Policy.
- **Right to data portability**: in accordance with Art. 20 GDPR, to receive the personal data concerning him or her, which he or she has provided to a controller in a structured, commonly used and machine-readable format or to have the right to transmit those data to another controller.
- **Right to withdraw consent**: in accordance with Art. 7 para. 3 GDPR, the right to withdraw his or her consent at any time. As a result, data processing based on this consent may not continue in the future. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. To exercise the right to withdraw, an informal notification via all known communication channels is sufficient. It shall be as easy to withdraw as to give consent.
- **Right to lodge a complaint with a competent supervisory authority**: to lodge a complaint with a competent supervisory authority in accordance with Art. 77 GDPR, in particular in the Member State of his or her habitual residence, place of work or the registered office of the members of the Festo Group or place of the alleged infringement.
- **Right to object**: to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1) GDPR, including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims. If the data subject wishes to exercise their right to object, an informal notification via all known communication channels is sufficient.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

9.4.1 Right of information

Where personal data relating to a data subject are collected from the data subject IArt. 13 GDPR) or have not been obtained from the data subject (Art. 14 GDPR), the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information.

The members of the Festo Group shall inform the data subjects who have rights as third-party beneficiaries in case of personal data collected from the data subject:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing is based;
- where the processing is based on point (f) of Article 6(1) GDPR, the legitimate interests pursued by the controller or by a third party;
- the recipients or categories of recipients of the personal data, if any;
- the fact that the controller intends to transfer personal data to a third country and the existence or absence of a sufficient standard of data protection (e.g. adequacy decision of the EU Commission, standard contractual clauses);
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability, the right to withdraw consent at any time and the right to lodge a complaint with a competent supervisory authority;
- the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- their rights as third-party beneficiaries pursuant to clause 11.6 as well as the options for exercising these rights, liability pursuant to clause 12 and the Data privacy principles pursuant to clause 9.1

Where personal data have not been obtained from the data subject, the members of the Festo Group shall provide the data subject additionally with the following information:

- the categories of personal data concerned
- from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

The information obligations do not exist, if

- the data subject already has the information,
- the provision of such information proves impossible or would involve a disproportionate effort,
- where the personal data must remain confidential subject to an obligation of professional secrecy or
- obtaining or disclosure is expressly laid down by Union or Member State law.

9.4.2 Right of access, rectification, erasure or restriction of processing of data

Data subjects have the right, on request:

- to receive information at reasonable intervals, in particular by means of personal information or a copy of all data relating to them that is processed. The members of the Festo Group will endeavor to provide the information free of charge within the legal requirements. If there is considerable expense involved, the Festo Group reserves the right to charge the costs incurred to the requester of the information, insofar as this is permitted by law.
- to have data corrected, erased or blocked, in particular if this data is incomplete or inaccurate.
- to object to the processing of their personal data, unless the processing of this data is required by law. Where the objection is justified, the processing must cease.
- to object free of preconditions to the processing of personal data concerning them for purposes of direct marketing.

To limit the expense incurred, the data subject is asked to specify the areas or data in question as precisely as possible. The rights of the data subject also apply in the absence of specification. Where required, each member of the Festo Group is obliged to nominate suitable persons as contact persons to exercise the rights of the data subjects and to make them transparent to employees and customers. Competent contact persons can be Data protection coordinators or Data protection officers, the legal department or other suitable persons as determined by the members of the Festo Group.

Questions can be sent to the e-mail addresses "datenschutz@festo.com", "dataprivacy@festo.com" or the service hotline (Service Center Tel. +49-711/347-2008).

9.4.3 Exemptions and restrictions

Transparency, information and access rights are restricted if this restriction is necessary

- to protect the public safety or the safety of the members of the Festo Group;
- to prevent, investigate, detect and prosecute criminal offences or abuses;
- to safeguard trade and enterprise secrets of the Festo Group;
- to protect the data subject and the rights and freedoms of others.

9.5 Automated individual decision-making, including profiling

The members of the Festo Group commit that no decision about data subjects which significantly affects them will be based solely on an automated processing of their personal data, including profiling, unless.

- the decision is necessary for the conclusion or performance of a contract between the data subject and the controller,
- the decision is authorized on the basis of legal requirements and these legal requirements contain appropriate measures to safeguard the rights and freedoms as well as the legitimate interests of the data subject or
- with the explicit consent of the data subject.

The decisions are not based on special categories of personal data according to Art. 9 para. 1 GDPR, unless Art. 9 para. 2 lit. a or g GDPR applies, and appropriate measures have been taken to protect the rights and freedoms of the data subject and his or her legitimate interests.

Suitable measures are taken to safeguard the legitimate interests of the data subject. These include especially

- the possibility of expressing your point of view personally to a specific contact person,
- the right to intervention by a natural person on the part of Festo
- and to contest the decision within the framework of the statutory requirements.

9.6 Security and confidentiality

The members of the Festo Group commit to implement appropriate technical and organizational measures in accordance with Art. 32, 24, 25 GDPR, which are based on the generally recognized protection objectives of IT security/information security, in particular confidentiality, integrity, availability, resilience, encryption, Data privacy by design, pseudonymization, etc. Taking into account the status of technology, the nature, scope, circumstances and purposes of the processing and the varying likelihood and severity of the risk to the rights and freedoms of natural persons, the members of the Festo Group shall document and implement a level of protection appropriate to the risk to the rights and freedoms of data subjects with regard to the necessary measures, which shall be ensured in particular by observing the Information security in accordance with Attachment 2.

Technical and organizational measures are implemented that are designed to ensure that the Data privacy principles and the requirements set out in the Policy are met in practice (Data privacy through technology design and through data protection-friendly default settings in accordance with Art. 25 GDPR).

The IT security concept is subject to a procedure for regularly reviewing, assessing and evaluating the effectiveness of the technical and organizational measures. The technical and organizational measures are subject to technical progress and further development, so that adequate alternative measures are always possible. The overall security level of the defined measures is not undercut. Significant changes must be documented.

When processing special categories of personal data, increased security measures, in particular encryption measures, must be provided.

10. Obligations of the Festo Group

The members of the Festo Group ensure that before transferring personal data to a third country, they assess the laws and practices of that third country that may affect the respect of the commitments contained in the BCR. In particular, the members of the Festo Group give due account to the following elements:

- The specific circumstances of the transfers or set of transfers, and of any envisaged onward transfers within the same third country or to another third country, including:
    - purposes for which the data is transferred and processed (e.g. marketing, HR, storage, IT support)
    - types of entities involved in the processing (the data importer and any further recipient of any onward transfer);
    - categories and format of the personal data transferred;
    - location of the processing, including storage; and
    - the transmission channels used.
- The laws and practices of the third country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorizing access by such authorities and those providing for access to these data during the transit between the country of the data exporter and the country of the data importer, as well as the applicable limitations and safeguards.
- Any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under the BCR, including measures applied during the transmission and to the processing of the personal data in the country of destination.

10.1 Internal data processors

The following principles ensure the protection of personal data when a processor is part of the Festo Group. The controller (data exporter) must select a data processor (data importer) who offers sufficient guarantees with regard to the technical measures and organizational precautions to be taken for the processing and must ensure compliance with these measures through the following structure of obligations. The controller must conclude a written or electronic contract with the processor in accordance with the legal provisions, in particular Art. 28 GDPR, in which at least the following is regulated:

- subject matter and duration of the processing,
- nature and purpose of the processing,
- the type of personal data,
- the categories of data subjects,
- the obligations and rights of the controller,
- Right of instruction of the controller obligation of confidentiality and professional secrecy of authorized persons,
- technical and organizational measures in accordance with Article 32 GDPR,
- Involvement of other processors,
- Support obligations of the processor regarding the rights of data subjects and compliance with the obligations pursuant to Art. 32 to 36 GDPR,
- Obligations of deletion and return after the end of the provision of services relating to processing
- Controller's information and inspection rights,

For the members of the Festo Group, the "group contract on the processing of personal data" applies.

10.2 Obligations of the data exporter

The data exporter agrees and warrants:

- That no transfer is made to a BCR member unless the BCR member is effectively bound by the BCR and can deliver compliance;
- to monitor, on an ongoing basis, and where appropriate in collaboration with data importers, developments in third countries to which the data exporters have transferred personal data that could affect the initial assessment of the level of protection and the decisions taken on such transfers;
- in the event that the level of protection in a third country is no longer adequate, to promptly identify along with the liable BCR member(s) and the relevant Data privacy organization supplementary measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the BCR member acting as data exporter and / or data importer, in order to enable them to fulfil their obligations under the BCR;
- to suspend the transfer or set of transfers at stake, where the BCR member acting as data exporter, along with the liable BCR member(s) and the relevant data privacy organization, asses that the BCR – even if accompanied by supplementary measures – cannot be complied with for a transfer or set of transfers, or if instructed by the competent authorities, as well as all transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the transfer is ended;
- to end the transfer or set of transfers if the BCR cannot be complied with and compliance with the BCR is not restored within one month of suspension. In this case, personal data that have been transferred prior to the suspension, and any copies thereof, must be returned or destroyed in their entirety.
- to inform all other BCR members of the assessment carried out and its results, so that the identified supplementary measures will be applied in case the same type of transfers is carried out by any other BCR member or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended;
- to process the personal data, including the transfer, in accordance with the relevant provisions of the applicable Data privacy law (and, where applicable, will be notified to the competent authorities of the Member State in which the data exporter is established) and does not infringe the relevant provisions of that State;

- to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons (Art. 35 GDPR);to consult the competent supervisory authority prior to processing where a data protection impact assessment under Art. 35 indicates that the processing would result in a high risk in the absence of measures taken by the data exporter to mitigate the risk (Art. 36 GDPR);
- to have instructed the data importer, and will instruct the data importer for the duration of the data processing services, to process the personal data transferred only on behalf of the data exporter and in accordance with applicable Data protection law and this Policy;
- to suspend data transfers if the data importer breaches the BCR, is unable to comply with them, or ceases to be a data importer. In that case, personal data transferred before the suspension and any copies thereof must be returned to the data importer or completely destroyed.
- to verify that the data importer provides sufficient guarantees with respect to the technical and organizational measures described in Attachment 2 to this Agreement;
- that the security measures are sufficient to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, taking into account the requirements of the applicable Data protection law, the state of the art, the cost of their implementation, the risks represented by the processing and the nature of the data to be protected;
- that in the case of the transfer of special categories of data, the data subject is informed, before or as soon as possible after the transfer that his or her data may be transferred to a third country, which does not ensure an adequate level of protection within the meaning of Art. 44 et seq. GDPR;
- to make available to the data subjects, this Policy on the internet, except for Appendix 2, and a general description of the security measures, and, where applicable, a copy of the contract for data processing services awarded to another processor pursuant to the Policy, unless the Policy or the contract contains internal business information, in which case such business information may be redacted;
- that where a processing contract is awarded to another processor, the personal data and the rights of the data subject are protected at least to the extent required of the data importer under this Policy;
- to ensure compliance with the above clauses, in particular the safety measures described in attachment 2.

10.3 Obligations of the data importer

10.3.1 Obligations towards the data exporter

The data importer agrees and warrants:

- to process personal data only on behalf of the data exporter and in compliance with its instructions and this Policy;
- to notify the data exporter promptly if it has reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the BCR. This notification should also be provided to the liable BCR member(s).
- that it has implemented the technical and organizational measures specified in Attachment 2 before processing the personal data transferred;
- to notify the data exporter promptly about
    - any accidental or unauthorized access
    - any requests received directly from the data subjects without responding to these requests, unless it has been otherwise authorized to do so;
- to deal properly with all requests from the data exporter relating to its processing of the transferred personal data and to abide by the advice of the competent supervisory authority with regard to the processing of the data transferred;
- to make available, at the data exporter's request its IT systems and related documentation necessary for the processing for the purpose of auditing the processing activities covered by the Policy. The audit may be carried out by the data exporter or by an external auditor selected by the data exporter (if necessary in consultation with the competent supervisory authority), who has the necessary qualifications and is bound by confidentiality;

- to inform the data exporter in advance of the assignment of a processing contract to another processor outside the Festo Group and has obtained the data exporter's prior written consent;
- to immediately send the data exporter a copy of the subcontract for data processing outside the Festo Group that it has concluded in accordance with this Policy;
- to keep, return, or delete the personal data received under the BCR when the data importer ceases to be bound by the BCR. If the data exporter and data importer agree that the data may be kept by the data importer, protection must be maintained in accordance with Chapter V GDPR;
- in case of non-compliance with the BCR at the choice of the data exporter to immediately return or delete the personal data that has been transferred under the BCR in its entirety. Until the data is deleted or returned, the data importer should continue to ensure compliance with the BCR. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer should warrant that it will continue to ensure compliance with the BCR and will only process the data to the extent and for as long as required under that local law.

10.3.2 Obligations towards data subjects

The data importer agrees and warrants that:

- it will make available to the data subjects this Policy on the internet and, where applicable, an existing contract for the subcontracting of processing to another processor, unless the Policy or the contract contains internal business information, in which case such business information may be deleted; Appendix 2 shall be replaced by a general description of the security measures if the data subject cannot obtain such a copy from the data exporter;

10.3.3 Obligations in the case of a legally binding government access request

The data importer will promptly notify the data exporter and, where possible, the data subject if it:

- receives a legally binding government access request under the laws of the country of destination, or another third country, for disclosure of personal data transferred pursuant to the BCR,
- becomes aware of any direct government access to personal data transferred pursuant to the BCR in accordance with the laws of the country of destination;

Such notification will include all information available to the data importer.

If prohibited from notifying the data exporter and/or the data subject, the data importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible and will document its best efforts in order to be able to demonstrate them upon request of the data exporter.

The data importer will review the legality of the request for disclosure and will challenge the request if, after careful assessment, it concludes that it is unlawful. When challenging a request, the data importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the personal data requested until required to do so under the applicable procedural rules.

The data importer will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

In any case, the transfers of personal data by a BCR member pursuant to a government access request cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

The data importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It will also make it available to the Competent supervisory authorities upon request.

The data importer will provide the BCR member acting as data exporter, at regular intervals, with as much relevant information as possible on the requests received. If the data importer is or becomes partially or completely prohibited from providing the data exporter with the aforementioned information, it will, without undue delay, inform the data exporter accordingly.

10.4 Data processing by external parties

The following restrictions apply to the data transfer and onward transfer of data-to-data processors and controllers not belonging to the Festo Group.

- For external data processors outside the Festo Group that are established within the EU or in a country with a level of Data privacy recognized as adequate by the EU Commission, a written agreement is required stating that they only act under the instructions of the controller and are responsible for implementing appropriate measures to ensure the security and confidentiality of data processing.
- When transferring data to external data controllers outside the EU, the EU regulations for cross-border data flows must be applied, e.g. by incorporating the adequacy decisions issued by the EU Commission, the EU standard contractual clauses or other appropriate measures pursuant to Article 44 et seq. GDPR.
- When transferring data to external processors outside the EU, in addition to the provisions for cross-border data flows pursuant to Article 44 et seq. GDPR, the provisions for data processors pursuant to Art. 28 GDPR must be observed.

11. Implementation of and compliance with the Policy

11.1 Training program

The members of the Festo Group commit to provide appropriate training for all employees who have permanent or regular access to personal data, who are involved in the collection of data or in the development of tools used to process personal data.
The training program within the Festo Group, in which the regulatory content of this Policy and the procedures of managing requests for access to personal data by public authorities are also integrated, are offered to employees in three different ways.

(1): In-house training with own content, own training academy
(2): Online training courses /e-learning: special training software, web-based training (WBT) on the intranet (WeNet)
(3): Comprehensive Data privacy information and training material prepared by the Festo Group is available on the intranet (WeNet); dedicated news channel on the intranet (WeNet) for current information - available on subscription, available for everyone

All employees charged in accordance with the regulations with collecting, processing or using personal data, e.g. from the HR department, must complete and provide evidence of having completed a suitable training in category (1) or (2) when they are newly hired and then at least every three years. The Data Privacy Officer may request ad-hoc trainings in all categories if there are substantial changes in practice of processing of personal data or applicability of this Policy.

11.2 Data privacy audit

The members of the Festo Group commit to carry out an appropriate data protection audit to ensure compliance with the Policy within the Festo Group; this audit shall have the following characteristics among others:

- The audit program is oriented towards module B 1.5 of the BSI as well as ISO 27000. The audit program covers all aspects of the Policy and establishes procedures to ensure that remedial action is taken if vulnerabilities and problems are discovered.
- Data privacy audits are carried out regularly every two years on a rolling basis in the various companies of the Festo Group by internal experts (Corporate Internal Audit - CA) or by external, suitable experts or at the request of the competent Data privacy officer (or another competent entity in the company concerned with data privacy).
- The audit results are communicated to the Data privacy officers and the management of the local branch and the parent company.
- The Data privacy authorities may request a copy of these audits.

- Each member of the Festo Group must tolerate these audits carried out by the Data privacy authorities and comply with their notifications and recommendations relating to the application of the Policy.

11.3 Data privacy organization

The Festo Group maintains a Data privacy organization consisting of the appointed Data privacy officers, (operational and regional) Data privacy coordinators and other competent persons within the Festo Group, who, with the support of the management, monitor and coordinate compliance with Data privacy regulations across the Group level.

In particular, the Data privacy organization is responsible for reviewing and ensuring compliance with this Policy. The members of the Data privacy organization of the Festo Group advise management and must be involved in investigations by the Data protection authorities. The Data privacy organization reports annually on the application of the Policy and ensures the necessary communication at group level.

The Data privacy officers, Data privacy coordinators and other competent persons report on significant Data privacy issues and incidents and work towards compliance with Data protection regulations at company level.

The Data privacy organization is headed by the Data privacy officer of Festo SE & Co. KG as speaker and coordinator, who is tasked with monitoring compliance with the Policy. Details of the Data privacy organization can be found in the document "Data privacy Organization" in Attachment 3.

Position of the Data privacy officer

The Data privacy officer

- is involved at an early stage in all issues relating to the protection of personal data.
- receives the resources and information necessary to perform its duties.
- is not subject to instructions in the performance of his or her duties and may not be dismissed or disadvantaged because of the performance of his or her duties
- reports directly to the highest management level of the controller or processor.
- may be directly contacted by data subjects for all Data privacy issues.
- in the performance of his or her duties, the Data Privacy Officer is to maintain confidentiality.

Tasks of the Data privacy officer

The Data privacy Officer is responsible for the following tasks:

- Informing and advising the controller, the processor and the employees carrying out the processing about their Data privacy obligations
- Monitoring compliance with Data protection regulations and the Data privacy policy of the controller or processor
- Cooperation with the supervisory authorities, direct contact for the supervisory authorities

The Data privacy officer should not have any tasks that could result in conflict of interests.

11.4 Conflict with national regulations

Existing country-specific legal obligations of the members of the Festo Group are not affected by this Policy and must always be given priority. The regulations contained in this Policy shall apply in instances where provisions on data protection contained in national or international law are less stringent.

The members of the Festo Group will only apply the BCR as a means of transferring data where they have determined that the laws and practices in the third country do not prevent them from complying with their obligations under these BCR. This is based on the understanding that the laws and practices respect the core of fundamental rights and freedoms and do not conflict with the BCR.

In cases where security measures beyond the BCR are to be taken, the responsible BCR members and the competent Data privacy function will be informed and involved in the assessment. BCR members are obliged to appropriately document such assessment as well as the supplementary measures selected and implemented. They must make such documentation available to the competent supervisory authority upon request.

11.5 Internal complaint handling process

The members of the Festo Group commit to introduce an internal complaints procedure that complies with the following principles:

- Each data subject can lodge a complaint on the grounds that a member of the Festo Group has breached the Policy.
- The complainant can submit his / her complaint verbally or in writing to the competent Data privacy officer, Data privacy coordinator or to Datenschutz@festo.com (=complaints office). A complete overview of the competent Data privacy officers is available on the Festo Group's WeNet portal.
- The complaint will be processed by the competent Data privacy organization and a decision is usually made within one month. In cases of high complexity and number of requests, the one-month period may be extended at maximum by two further months, in which case the complainant should be informed accordingly within one month of receipt. The competent Data privacy organization has an appropriate degree of independence in the performance of its duties as a complaints office.
- The data subject also has the right to appeal to the Data privacy officer of the Festo SE & Co KG regarding the decision of the Data privacy organization. In addition, the data subject may appeal to the competent authorities and courts in accordance with his or her obligations under labor law.

11.6 Third-party beneficiary enforceable by data subjects

This Policy confer rights to data subjects to enforce the Policy as third-party beneficiaries as regards

- the basic requirements of clause 9,
- obligations in case of local laws and practices affecting compliance with the BCR (clause 10.3.1) and in case of government access requests (clause 10.3.3),
- the cooperation duties with the competent supervisory authorities (clause 13),
- the duty to inform the data subjects about any update of the BCR and of the list of BCR members pursuant clause 14 by publishing the new version without undue delay

and the following elements.

The data subjects can enforce against the data exporter their legal positions as third-party beneficiaries established by the Policy (in particular clauses 5, 9.4 et seq., 10., 10.4, 11.5, 12.).

Data subjects can enforce against the data importer their legal positions as third-party beneficiaries established by this Policy in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

The data subjects can enforce against the sub-processor their legal positions as third-party beneficiaries established by this Policy in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing activities under the Policy and the concluded service agreements.

This third-party beneficiary clause is limited to personal data originating from the European Union and transferred from the European Union to third countries.

The members of the Festo Group do not object to the data subject being represented by an association or other body appointed to exercise his or her Data privacy rights in accordance with national law, provided that he or she expressly requests this, and national law permits it.

This Policy grants the data subjects enforcement rights as third-party beneficiaries. This includes the right to judicial remedies and the right to obtain redress and, where appropriate, compensation in case of any breach of one of the enforceable elements of the BCR. for any the rights the right to receive compensation as per (Art. 77 – 82 GDPR).

The data subject has the right to lodge a complaint:

- before the competent court of the EU Member States where the controller, the processor or the liable parent company has an establishment, or where the data subject has his or her habitual residence and
- with a competent supervisory authority, in particular in the Member State of the data subject's habitual residence, place of work or place of the alleged infringement.

The members of the Festo Group commit to make this clause on third-party beneficiaries available to all data subjects with third-party beneficiary rights as per clause no. 5 (transparency). This Policy will be published on the Internet.

12. Centralized responsibility and liability regime

The respective most direct European parent company of an affected member of the Festo Group outside the EEA, which is specifically determined for each member of the Festo Group in Attachment 1.2, accepts liability for and agrees to take the necessary actions to remedy the acts of this member of the Festo Group and to pay compensation for any material or non-material damages resulting from the violation of the Policy by this member of the Festo Group.

This liability clause is limited to personal data originating from the European Union or transferred from the European Union to third countries.

The burden of proof rests with the above-mentioned parent company of the Festo Group member concerned, i.e. it is up to it to prove that the member of the Festo Group outside the EU is not liable for the breach of the Policy resulting in the damages claimed by the data subject. If the parent company can prove that the member of the Festo Group outside the EU is not liable for the breach, it may discharge itself from any liability.

13. Cooperation with supervisory authorities

The members of the Festo Group ensure to cooperate with, to accept to be audited and to be inspected, including where necessary, on-site, by the competent supervisory authorities,

- to take into account their advice, and
- to abide by decisions of these supervisory authorities

on any issue related to the BCR.

The data exporter agrees to deposit a copy of this Policy with the competent supervisory authority if it so requests or if such deposit is required under the applicable Data protection law.

The parties agree that the competent supervisory authority is authorized to audit the data importer and any other processors, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable Data protection law.

14. Updating the regulations

The Festo Group has to keep the BCR up to date in order to reflect the current situation, for instance to take into account modifications of the regulatory environment, in compliance with Art. 47 GDPR and the EDPB Recommendations, or changes to the scope of the BCR.

The Festo Group is obliged to report changes, including to the list of BCR members, without undue delay, to all BCR members.

The "Corporate Legal Department" keeps a fully updated list of the BCR members, which serves as the basis for Attachment 1.2 "CA 0741 Members of the Festo Group" of this Policy.

The Data privacy organization "Global Data privacy " keeps record of any updates to the BCR, and provides the necessary information to data subjects, and upon request, to competent supervisory authorities.

Once a year, the supervisory authorities should be notified via the Management Board of the Festo SE & Co. KG of any changes to the BCR or to the list of BCR members in accordance with Attachment 1.2, with the brief explanation of the reasons for the changes.

The coordinator of the Data privacy organization in accordance with Attachment 3 and the contact person of the "Corporate Legal Department" shall come to an agreement about new members of the Festo Group, as well as significant changes to this Policy. Significant changes that affect the level of protection of the Policy must be communicated in advance by the coordinator of the Data privacy organization in accordance with Attachment 3 to the competent Data privacy authority, with a brief explanation of the reasons for the update.

15. Final provisions

In any case, data shall be processed in accordance with the applicable EU law and the relevant national regulations.

This Policy shall become binding across the group for the entire Festo Group as per CA 0741 Members of the Festo Groupe following an appropriate decision by the Management Board of Festo SE & Co. KG.

This Policy shall become binding for the members of the Festo Group across the Group in accordance with Attachment 1.2 following an appropriate decision by the Management Board of the Festo SE & Co. KG and by signing the declaration of commitment of the respective member of the Festo Group in accordance with Attachment 1.2.

The individual members of the Festo Group agree to obligate all employees who handle personal data to comply with this Policy and to include corresponding clauses in the existing declarations of commitment.