Viega Group's
Binding Corporate Rules
on data protection

Version: V1

Date: 1st April 2025

Table of Contents

Preamble 5
1. Definitions 6
1.1. Applicable data protection law 6
1.2. BCR member 6
1.3. (Competent) Supervisory authority 6
1.4. Consent 6
1.5. Controller 6
1.6. Data exporter 6
1.7. Data importer 6
1.8. Data Protection Management System (DPMS) 7
1.9. Data subject 7
1.10. Filing system 7
1.11. Lead supervisory authority 7
1.12. Member state 7
1.13. Personal data 7
1.14. Personal data breach 7
1.15. Processing 8
1.16. Processor 8
1.17. Profiling 8
1.18. Pseudonymisation 8
1.19. Recipient 8
1.20. Special categories of personal data 8
1.21. Third party 9
2. Scope of application 9
2.1. Territorial scope 9
2.2. Material scope 9
3. Binding nature of the BCR 10
4. Third party beneficiary rights 10
5. Data protection organisation 10
5.1. Data Protection Manager 10
5.2. Data Protection Officer 11
5.3. Data Protection Coordinators 11
6. Data protection principles 11
6.2. Fairness and transparency 13
6.3. Purpose limitation 13
6.4. Data minimisation 14

6.5. Accuracy 14
6.6. Storage limitation 14
6.7. Integrity and confidentiality 15
6.8. Accountability 15
6.8.1. Data processing on behalf 15
6.8.2. Record of processing activities 16
6.8.3. Data protection impact assessment 17
6.8.4. Data security 17
6.8.5. Notification of a personal data breach 18
6.8.6. Confidentiality of data processing 18
7. Transfer of personal data 18
7.1. Transfer of personal data between BCR members 18
7.2. Transfer of personal data from a BCR member to a non-BCR member or a third party within the EEA 19
7.3. Transfer of personal data from a BCR member to a non-BCR member or a third party outside the EEA 19
7.4. Transfer of personal data from a non-EEA based BCR member to a public authority in its country 20
8. Rights of data subjects 21
8.1. Right of information 21
8.2. Right of access 21
8.3. Right to rectification 22
8.4. Right to erasure 22
8.5. Right to restriction of processing 22
8.6. Right to data portability 23
8.7. Right to object 23
8.8. Right to lodge a complaint 23
8.9. Right of an effective judicial remedy 23
8.10. Right not to be subject to automated decision making 24
9. Compliance with these BCR 24
9.1. Dealing with complaints 24
9.2. Cooperation with supervisory authorities 25
9.3. Liability 25
9.4. Access to these BCR 26
9.5. Training of employees 26
9.6. Monitoring 26
10. Application and conflict of laws and regulations 27
10.1. General conditions 27
10.2. Local laws and practices affecting compliance with these BCR when transferring personal data 28

11. Final provisions 30
11.1. Document validity 30
11.2. Joining and leaving these BCR 30
11.3. Updates of these BCR 30

Appendix 1: Name and contact details of the Data Protection Manager and the Data Protection Officer

Appendix 2: List of parties bound by the BCR

Appendix 3: Nature of personal data transferred

Appendix 4: List of Changes (empty)

Appendix 5: Declaration of Accession (not included in public release)

Preamble

Viega is an internationally active group of companies that wants to offer its customers - wholesalers, specialist tradesmen, planners, architects, and consumers – a groupwide identical appearance, regardless of where the customer is located in the world. To achieve this, the IT systems and processes are developed and managed centrally. This sometimes also requires personal data to be transferred around the world. Much of the personal customer data is processed in the European Economic Area (“EEA”) - especially in Germany and Ireland - as well as in Switzerland. The Binding Corporate Rules, which Viega has adopted, ensure that data is processed under the same conditions even when it leaves the EEA.

The aim of these Binding Corporate Rules (hereinafter referred to as "BCR") of the Viega group of companies (hereinafter referred to as "Viega Group") is to ensure that personal data is processed in the data protection understanding of the European Union. This requires the establishment of uniform data protection and data security standards for the processing of personal data in all companies of the Viega Group, especially those residing outside the EEA, the so called third countries within the meaning of the EU Regulation 2016/679 General Data Protection Regulation (“GDPR”).

We ensure that the required level of data protection is also achieved in companies of the Viega Group based in these countries and that sufficient guarantees are provided with regard to the protection of personal rights and the exercise of corresponding rights in accordance with these BCR.

Viega GmbH & Co. KG is responsible for the proper implementation of these BCR within the Group. It obliges each participating member of the Viega Group, including its employees, to comply with these BCR. These BCR as well as all other policies and standards concerning data protection are available to the employees of the participating companies on the intranet at any time.

1. Definitions

1.1. Applicable data protection law

Applicable data protection law refers to any EEA data protection regulation that may apply to the processing of personal data by the Viega Group and/or a third party and, in particular, (i) the GDPR, and (ii) any other applicable regulation relating to the processing of personal data. For sake of clarity, with respect to Viega entities established outside the EEA receiving personal data under these BCR, the applicable data protection law shall be the one of the country of the Viega Group entity established in the EEA exporting the relevant personal data.

1.2. BCR member

A *BCR member* is a company of the Viega Group bound by this BCR regardless of whether it is located inside the EEA or outside it.

1.3. (Competent) Supervisory authority

Supervisory authority means an independent public authority for Data Protection which is established by a *Member State* of the EEA. Each supervisory authority shall be *competent* for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with the GDPR on the territory of its own Member State.

For the BCR members outside the EEA, the competent supervisory authority is the supervisory authority of the *data exporter* in the EEA.

1.4. Consent

Consent of the data subject means 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.

1.5. Controller

Controller means 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.

1.6. Data exporter

A *data exporter* is a BCR member that transfers personal data to another BCR member.

1.7. Data importer

A *data importer* is a BCR member that obtains personal data from a *data exporter*.

1.8. Data Protection Management System (DPMS)

The Viega Group's *Data Protection Management System* consists of policies, processes, standards, associated resources and activities that are systematically created, controlled, and monitored. The aim of the DPMS is to ensure the protection of the fundamental rights and freedoms of natural persons when processing personal data. The basis of the DPMS is the GDPR.

The Data Protection Manager of the Viega Group operates the DPMS.

1.9. Data subject

A *data subject* is an identified or identifiable natural person.

1.10. Filing system

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

1.11. Lead supervisory authority

Lead supervisory authority refers to the supervisory authority competent for the cross-border processing carried out by the Viega Group, i.e. Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW).

1.12. Member state

A *member state* is a state that is member of the European Union. Current member states are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.

In these BCR also the European Free Trade Association (EFTA) members Island, Liechtenstein, and Norway are included in the term member state.

1.13. Personal data

Personal data means any information relating to a *data subject*. An identifiable natural person is one 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.

1.14. Personal data breach

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.15. Processing

Processing means 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.16. Processor

Processor means a natural or legal person, public authority, agency, or other body which processes *personal data* on behalf of the *controller*.

1.17. Profiling

Profiling means any form of automated processing of *personal data* consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

1.18. Pseudonymisation

Pseudonymisation means 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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

1.19. Recipient

Recipient means 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 based in the EEA which may receive *personal data* in the framework of a particular inquiry in accordance with European 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 laws according to the purposes of the processing.

1.20. Special categories of personal data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership are referred to as *special categories of personal data*. 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 are also classified as special categories of *personal data*.

1.21. Third party

Third party means 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 authorised to process *personal data*.

2. Scope of application

2.1. Territorial scope

These BCR apply in the following scenarios:

- when EEA-based BCR members process personal data, and these data are then transferred to a non-EEA-based BCR member.
- when non-EEA-based BCR members process personal data, and these data are then transferred to another BCR member.
- when a non-EEA-based BCR member processes personal data further, and these data were initially transferred by any other BCR member.
- When non-EEA-based BCR members transfer personal data to a recipient outside the EEA, and these data were initially transferred by a BCR member.

These BCR do not apply to any processing of personal data by a non-EEA-based BCR member where such processing:

- does not concern personal data having been initially transferred by a BCR member bound by the GDPR
- concerns personal data of a data subject outside the EEA and
- is only conducted by this BCR member and its processors.

2.2. Material scope

These BCR apply to

- the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system,
- those BCR members which are processing personal data in their capacity as (internal) processors on behalf of another BCR member; however only to the extent they do not lead to a contradiction of a respectively concluded agreement,
- the processing of personal data by each BCR member listed in **Appendix 2**,
- the processing activities set out in **Appendix 3**.

3. Binding nature of the BCR

These BCR are legally binding for each BCR member and its employees. Each BCR member and each of its employees is obliged to respect the principles and obligations laid down in these BCR. The binding nature of the BCR encompasses:

- *Binding nature for BCR members* – The Viega Group has introduced the BCR within the BCR members and set up a mechanism to make these BCR binding upon any BCR member listed in **Appendix 2**. Each Viega entity has contractually bound itself to adhere to the principles of the BCR by signing the Intergroup Agreement with all participating parties. Where this is necessary for the BCR to be effective, each BCR member is obliged to implement all additional requirements to make the BCR binding as contractually required.
- *Binding nature for employees* – Employees are obliged to respect the principles laid down in these BCR as a result of their general obligations arising from their employment contract to comply with corporate policies. The enforcement of the BCR and potential sanctions of any violations of the BCR vis-á-vis employees are ensured by the internal compliance structure. Where this is necessary for the BCR to have such binding effect vis-á-vis the respective employees, each BCR member is obliged to implement all additional requirements to make the BCR binding as contractually required.

4. Third party beneficiary rights

Individuals are third party beneficiaries and can derivate rights from these BCR.

All BCR members commit to granting individuals third party beneficiary rights under these BCR in respect of the processing of their personal data. Accordingly, it is expressly acknowledged and accepted by each BCR member that data subjects will be entitled to enforce the provisions of clauses 3, 4, 6, 7, 8, 9.1.1. - 9.1.4., 10, 11.3. of these BCR in respect of the processing of their personal data.

5. Data protection organisation

The Viega Group has established a structured data protection organisation in which roles and responsibilities have been defined. This is intended to provide an appropriate support framework to ensure the lawful processing of personal data within the Viega Group.

5.1. Data Protection Manager

The Viega Group appointed a Data Protection Manager (DPM) located within the European Union to operate the DPMS and monitor the compliance of the BCR members to these BCR. The DPM is also responsible for the DPMS and the risk management for data protection risks and processes. The DPM

informs and advises the group board of directors, deals with supervisory authorities' investigations, monitors and annually reports on compliance at a global level.

The name and contact details of the DPM can be found in **Appendix 1** and are published on the Internet at https://viega.com/privacy.

5.2. Data Protection Officer

The Data Protection Officer (DPO) is, on the one hand, an advisor to the management on all matters of data protection and, on the other hand, a contact person for the supervisory authorities. The tasks of the DPO are derived from the GDPR. The DPO reports directly to the management of the liable BCR member and informs them if any questions or problems arise during the performance of their duties. A DPO has been appointed for the German entities and is registered with the responsible supervisory authority. A BCR member designates a DPO in any case where the core activities of the BCR member consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.

The name and contact details of the DPO can be found in **Appendix 1** and are published on the Internet at https://viega.com/privacy.

5.3. Data Protection Coordinators

Each BCR member shall appoint a Data Protection Coordinator (DPC). DPCs are contact persons for the DPM. They also support the so-called Risk Owners (employees responsible for specific tasks and processes) in identifying and planning measures for data protection risks and supporting the DPM in monitoring the effectiveness of the implemented measures. The DPCs may handle local complaints from data subjects, reporting major privacy issues to the DPM, monitoring training and compliance at their local entity. A DPC may be appointed by more than one BCR member, provided that the Coordinator is authorised to represent the company and can be easily reached by any of these employees.

6. Data protection principles

BCR members respect the importance of individual's privacy. When personal data held by BCR members is processed, the fundamental rights and freedoms of data subjects, in particular their right to the protection of personal data, must be respected.

When processing personal data, the companies of the Viega Group always comply with the following principles:

6.1. Lawfulness

Personal data may only be processed in a lawful manner. There must be a legal basis for any processing of personal data. Processing is only permitted if at least one of the following conditions is met:

- The data subject has given consent to the processing of personal data concerning him or her for one or more specific purposes.
  Consent may only be given on a voluntary basis. The data subject shall be informed in advance of the specific processing activity in an intelligible and easily accessible form. The data subject must have the possibility to informally withdraw consent at any time.
- The 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.
- The processing is necessary for compliance with a legal obligation to which the controller is subject.
- The processing is necessary to protect the vital interests of the data subject or another natural person.
- The processing is necessary to protect the legitimate interests of a BCR member or a third party, unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.
- The processing of personal data of employees is permitted under the data protection or other relevant laws applicable in the EEA countries.

The processing of personal data relating to criminal convictions and offences or related security measures based on one of the legal bases mentioned above will be carried out only under the control of a official authority or when the processing is authorised by European Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Section 10 remains unaffected.
The processing of special categories of personal data is not permitted. The processing of such data is exceptionally allowed if there is a legal basis mentioned above and additionally one of the following applies:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
- the data subject is unable to give consent (e.g. in a medical emergency) and the data processing is necessary to protect the vital interests of the individual;
- the processing relates to personal data which are manifestly made public by the data subject; or
- processing is necessary for the establishment, exercise or defence of legal claims, where there is no reason to assume that the data subject's legitimate interests would be of overriding importance such as to prevent the processing.

The DPM and, if appointed for the company concerned, the DPO shall be consulted prior to the introduction or performance of processing activities involving special categories of personal data.

6.2. Fairness and transparency

Personal data must be processed in a fair and transparent manner in relation to the data subject. This means that data subjects will generally be adequately informed at the time of collection of their personal data. Where personal data relating to a data subject are collected from the data subject, the controller shall provide the data subject with all of the following information:

- the identity and contact details of the BCR member acting as Controller;
- the contact details of the DPM and, if appointed, the DPO;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the categories of personal data concerned;
- where applicable, the legitimate interests pursued by the controller or by a third party;
- the recipients or categories of recipients of personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the European Commissioner or the reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
- the period for which the personal data will be stored or, if this is not possible, the criteria used to determine this period;
- the existence of the rights of data subjects under section 8;
- where the processing is based on a consent of the data subject, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- the existence of automated decision-making, including profiling, and, at least in such cases, meaningful information about the logic involved and the significance and envisaged consequences of such processing for the data subject.

If, exceptionally, personal data have not been collected from the data subject, the Controller shall provide information to the same extent as described above. In addition, the Controller shall indicate from which source the personal data originate, and if applicable, whether it came from publicly accessible sources.

6.3. Purpose limitation

Personal data may only be collected for specified, explicit and legitimate purposes. It may not be processed in a way that is incompatible with those purposes, unless the change of purpose is permitted by EU Data Protection Law. Additional measures are taken to protect the rights and freedoms of the data

subject such as the consent of the respectively data subjects, limiting access to the personal data, additional confidentiality and security controls, provision of information to the data subject.

Generally permitted purposes for further processing, which are deemed compatible with the original purpose are archiving and internal audit and investigations.

In order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, inter alia, the following must be taken into account:

- any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the BCR member;
- the nature of the personal data, in particular whether special categories of personal data are processed or whether personal data related to criminal convictions and offences are processed (see above 6.1);
- the possible consequences of the intended further processing for data subjects;
- the existence of appropriate safeguards, which may include encryption or pseudonymisation.

The DPM will provide guidance as to if and when such change is permitted. In case of a permitted change of purpose, data subjects must be informed of any such changes in accordance with section 6.2.

6.4. Data minimisation

The processing of personal data must be adequate, relevant and limited to what is necessary for the purposes of the processing.

6.5. Accuracy

Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay.

6.6. Storage limitation

Each BCR member will keep personal data no longer than necessary for the purpose the personal data is processed, without prejudice to rules set forth in the section 10 of these BCR. If personal data must be retained for other reasons than its original purpose (e.g. because applicable national laws require to keep the data for a longer period of time) the access to it will be restricted. Once there is no legal or legitimate interest to retain the personal data by the BCR member anymore, the personal data will be anonymised or securely deleted.

6.7. Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by appropriate technical and organisational measures.

6.8. Accountability

Every BCR member shall be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with these BCR, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

6.8.1. Data processing on behalf

Viega Group uses processors on a contractual basis to perform various activities. In doing so, Viega only uses processors who offer sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of these BCR and ensure the protection of the rights of the data subject.

Any processing by a processor will be governed by a contract or other legal act that is binding on the processor regarding the controller stipulating among others:

- processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation;
- ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- takes all measures required pursuant to section 6.8.4;
- respects the conditions mentioned below for engaging another processor;
- taking into account the nature of the processing, assists the controller, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in section 8;
- assists the controller in ensuring compliance with the obligations under data protection law taking into account the nature of processing and the information available to the processor;
- at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless laws require storage of the personal data;
- makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this section and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

The processor shall immediately inform the controller if, in its opinion, an instruction infringes applicable data protection law.

The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract between the controller and the processor shall be imposed on that other processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of these BCR. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

To demonstrate sufficient guarantees as referred to in this section, a code of conduct, a data protection certification, standard contractual clauses can be used.

Any contract shall be in writing, including in electronic form.

6.8.2. Record of processing activities

Each BCR member acting as a Controller must keep all processing activities in a common register of processing activities. That register contains at least the following information for each processing activity:

- the name and contact details of the Controller and, where applicable, the joint controller, the controller's representative and the DPO, if any;
- 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 organisations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, if necessary, the documentation of suitable safeguards as defined in section 7.3;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures.

Each BCR member acting as a Processor shall maintain a record of all categories of processing activities carried out on behalf of a Controller. That register contains at least the following information for each processing activity:

- the name and contact details of the Processor or Processors and of each controller on behalf of which the Processor is acting, and, where applicable, of the Controller's or the Processor's representative, and the DPO, if any;
- the categories of processing carried out on behalf of each Controller;

- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, if necessary, the documentation of suitable safeguards as defined in section 7.3;
- where possible, a general description of the technical and organisational security measures.

The records shall be maintained in writing, including in electronic form, and must be made available to the competent supervisory authority on request.

The DPM defines the requirements for the directory and provides templates and other assistance to BCR members. The information is checked regularly by the respective DPC and supplemented if necessary.

6.8.3. Data protection impact assessment

Where a processing activity is likely to result in a high risk to the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing, the controller is obliged to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. The DPM provides templates and other assistance for this purpose. If a data protection impact assessment shows that the processing would lead to a high risk and the Controller does not take measures to mitigate the risk, the Controller shall not start the processing and shall consult the competent supervisory authority prior to the processing.

6.8.4. Data security

The Viega Group processes personal data on the one hand in accordance with the internal guidelines and standards for information security and data protection and on the other hand in accordance with relevant laws and regulations.

Each BCR member will take appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data transmitted, stored or otherwise processed. Those measures include principles of data protection through technical design (data protection by design) and they ensure that, by default, each BCR member only collects and processes the personal data that is necessary for their business purposes (data protection by default).

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Viega has implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.8.5. Notification of a personal data breach

All BCR members undertake to inform their local data protection representatives (DPO / DPC) and the DPM immediately of any (suspected) breach of personal data within the scope of these BCR. This also applies to personal data breaches at external processors. In addition, the following notification obligations exist in case of such a personal data breach:

- The Controller shall notify the personal data breach to the competent supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.
- Any BCR member, operating as Processor for another BCR member shall notify any personal data breach to the respective BCR member operating as Controller and the relevant DPC.
- Where a personal data breach is likely to result in a high risk to the rights and freedoms of the affected data subjects, the BCR member shall communicate the personal data breach to them without undue delay.

Each BCR member will document such occurring breach of security (comprising the facts relating to the breach, its effects and the remedial action taken) and after consultation with the DPM / DPO make such documentation available to supervisory authorities upon request.

6.8.6. Confidentiality of data processing

Only authorised employees who have undertaken to comply with data protection may process personal data. It is prohibited to use the personal data entrusted within the scope of the activity for one's own private purposes, to transmit it to unauthorised persons or to make it accessible to them in any other way. Unauthorised persons in this sense are also employees who do not need the data to carry out the tasks incumbent upon them.

Each BCR member takes steps to ensure that any natural person acting under the authority of Viega who has access to personal data does not process them except on instructions from the BCR member.

7. Transfer of personal data

In order to fulfill orders from customers, personal data mentioned in **Appendix 3** will be transferred to other Viega entities or processors engaged by Viega entities.

7.1. Transfer of personal data between BCR members

The transfer of personal data between BCR members, especially if the receiving member resides outside the EEA, is only permitted if the receiving member fully complies to these BCR and local laws and

practices do not affect compliance with the BCR (see section 10). Transfer of personal data to non-compliant, resigned and expulsed members is not permitted. If compliance is not restored within one month of suspension, the data importer is in substantial or persistent breach of the BCR or the data importer fails to comply with a binding decision of a competent court or competent supervisory authority regarding its obligations under these BCR, section 11.2. applies.

7.2. Transfer of personal data from a BCR member to a non-BCR member or a third party within the EEA

The transfer of personal data from a BCR member to a non-BCR member of the Viega Group or a third party within the EEA is only permitted under the following aspects:

- Where the receiving entity is a processor, the conditions set out in section 6.8.1 must be met.
- Where the receiving entity is a controller which jointly determines the purposes and means of the processing with a BCR member, the requirements laid down in section 6.8.1 shall be met.
- Provided that the receiving entity is an independent data controller, it must demonstrate compliance with the relevant data protection laws and the maintenance of the level of data protection, unless it is a government entity.

7.3. Transfer of personal data from a BCR member to a non-BCR member or a third party outside the EEA

The transfer of personal data from a BCR member to a non-BCR member of the Viega Group or a third party **outside the EEA** is only permitted if the conditions for a transfer are met and local laws and practices do not affect compliance with these BCR (see section 10).

To enable the transfer of personal data, the third country of the receiving entity or the receiving entity itself ensures an adequate level of protection of personal data, provided by:

- an adequacy decision of the European Commission, stating that the third country, a territory or one or more specified sectors within that third country or the international organisation in question ensures an adequate level of protection;
- if the recipient has provided appropriate safeguards and on condition that enforceable individual rights and effective legal remedies are available to the data subjects; e.g. by virtue of standard contractual clauses adopted by the European Commission;

In the absence of an adequacy decision or of appropriate safeguards, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

7.4. Transfer of personal data from a non-EEA based BCR member to a public authority in its country

In case of a legally binding request by a public authority under the laws of the country of destination, or of another third country, for disclosure of personal data transferred pursuant to these BCR, the affected BCR member will promptly notify the data exporter and, where possible, the data subject. Such notification will include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided.

If a BCR member becomes aware of any direct access by public authorities to personal data transferred pursuant to these BCR in accordance with the laws of the country of destination, the BCR member will promptly notify the data exporter and, where possible, the data subject. Such notification will include all information available to the BCR member.

The BCR member will use its best efforts to be able to communicate as much information as possible and as soon as possible to other affected BCR members and data subjects.

The data importer will preserve the abovementioned information for as long as the personal data are subject to the safeguards provided by these BCR, and shall make it available to the competent supervisory authorities upon request.

The BCR member acting as a data importer will provide the BCR member acting as a data exporter with regular and as detailed information as possible on requests received from public authorities. In case the transfer of such information is partially or completely prohibited, the BCR member shall inform the data exporter accordingly without undue delay.

Before providing the requested information, the BCR member shall assess whether the request is in accordance with the law of the country of destination, applicable obligations under international law and the principles of international comity. If there is any doubt as to the legality, the BCR member shall challenge the request and shall not disclose the requested personal data until it is required to do so under the applicable procedural rules. This legal assessment will be documented and made available to the data exporter and the competent supervisory authorities by request. In any case, the data importer

will only provide the minimum amount of information permissible to public authorities. Transfers of personal data by a BCR member to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

8. Rights of data subjects

Every data subject, regardless of his or her place of residence and regardless of the place of processing, has the following inalienable rights with regard to his or her personal data processed by a BCR member under the condition of these BCR. Data subjects must not be disadvantaged in any way as a result of exercising their rights.

Any request that a BCR member may receive from a data subject in relation to the data subject's rights set forth in this section will be handled in accordance with the BCR complaint handling procedure described in section 9.1.

8.1. Right of information

The data subject has the right of information of how his or her data is processed by the BCR members as described in 6.2. The right of information includes also the right for every data subject to have an easy access to the latest version of these BCR as described in section 9.4.

8.2. Right of access

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and information like the purposes of the processing, the categories of personal data concerned and the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations. Where possible, the envisaged period for which the personal data will be stored should be indicated and, if this is not possible, the criteria used to determine that period. The data subject receives information on the existence of the right to obtain from the controller the rectification or erasure of personal data concerning the data subject or the restriction of the processing of such data or to object to the processing, as well as on the data subject's right to lodge a complaint with a supervisory authority. If the personal data are not collected from the data subject, the data subject shall be provided with all available information as to their source. The data subject will be informed about 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.

In addition, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer where personal data are transferred to a third country or to an international organisation.

The controller shall provide a copy of the personal data undergoing processing.

8.3. Right to rectification

The data subject has the right to obtain rectification of inaccurate personal data relating to him or her processed by a BCR member without undue delay and to have incomplete personal data completed, taking into account the purposes of the processing, including by means of providing a supplementary statement.

8.4. Right to erasure

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay when one of the following grounds applies: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing; the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes; the personal data have been unlawfully processed; the personal data have to be erased for compliance with a legal obligation in European Union or Member State law to which the controller is subject. Existing data retention obligations and/or conflicting interests must be observed; section 10 applies.

8.5. Right to restriction of processing

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject. If neither its accuracy nor its inaccuracy can be ascertained or if the processing does not comply with the provisions of these BCR or national legislation the processing of this personal information will be prohibited.

Where processing has been restricted in accordance with the above conditions, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or of a Member State.

A data subject who has obtained restriction of processing in accordance with the above conditions shall be informed by the controller before the restriction of processing is lifted.

8.6. Right to data portability

Where personal data have been provided by the data subject and the processing is based on the data subject's consent or on a contract with the data subject and the processing is carried out by automated means, the data subject has the right to receive their personal data in a commonly used and machine-readable format and to transmit those data (as technical possible) without hindrance to enable the data subject to use similar services from another controller.

In exercising the right to data portability, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The exercise of this right shall be without prejudice to Section 8.4. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The right to data portability shall not adversely affect the rights and freedoms of others.

8.7. Right to object

The data subject shall have the right 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 the legitimate interests of the controller. The right to object must be taken into account if a review of the facts shows that, due to special personal circumstances, an interest of the data subject worthy of protection is more important than the interests of the data controller. Where personal data are processed for direct marketing purposes, or statistical purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her.

8.8. Right to lodge a complaint

The data subject has the right to lodge a complaint with any supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes these BCR. The BCR members grant the collaboration with the supervisory authorities.

Furthermore, the data subject has the right to contact the DPM or – if appointed – the DPO to lodge a complaint against the processing of a BCR member through the internal complaint mechanism of the Viega Group as described in 9.1.

8.9. Right of an effective judicial remedy

Each data subject shall have the right to an effective judicial remedy before a competent court in the EU when he or she considers that his or her rights under these BCR have been infringed as a result of the processing of his or her personal data in non-compliance with these BCR or the applicable data protection laws. This can either be the country of residence, the country of work or the courts where the BCR member resides. The BCR members accept that data subjects may be represented by a not-for-profit

body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf. This right also includes to obtain redress and, where appropriate, compensation in case of any breach of one of the enforceable rights of these BCR. The rules for liability are described in 9.3.

8.10. Right not to be subject to automated decision making

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. An exception applies in the following cases:

- the decision is necessary for entering into, or performance of a contract between the data subject and a controller;
- the decision is authorised by European Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests;
- the decision is based on the data subject's explicit consent.

The data subject's rights and freedoms and legitimate interests must be guaranteed by suitable measures, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

9. Compliance with these BCR

9.1. Dealing with complaints

Each data subject is entitled to claim violation of the BCR, address its individual rights as set out in section 8 of these BCR, enforce any other right of the BCR, or issue any other request to the data protection organisation.

Any data subject may contact the DPM or – if appointed – the DPO at any time with the aforementioned issues. Complaints can be submitted through several channels. The direct contact details can be found in **Appendix 1**. Further communication channels are published on the websites of the Viega Group and on the internal websites with all necessary information.

The receipt of the complaint shall be confirmed to the data subject in a timely manner and the complaint shall be answered without undue delay and in any event within one month from the receipt of the complaint. Taking into account the complexity and number of the requests, that one month period may be extended at maximum by two further months, in which case the data subject will be informed within one month from the receipt of the complaint. The staff members dealing with the complaint have a sufficient

degree of independence in the performance of this task. This is guaranteed by the fact that they are not involved in the data processing operations subject to the complaint.

Complaints that are abusive, especially if they are manifestly unfounded or excessive, in particular because of their repetitive character, or which constitute of insulting actions against Viega or any employee will be rejected. In such an event, the data subject will be provided in writing with an explanation of the reason for the refusal and granted the right to appeal.

In case the complaint is considered justified, the BCR member will take adequate action(s) to address the complaint with reasonable efforts to rectify and remedy the situation that gave rise to the complaint. The data subject will be notified in writing that adequate action(s) to address the complaint will be or have been initiated. In any case, the data subject will be notified about his or her right to lodge a claim before a court or a complaint before a supervisory authority in accordance with section 9.3. in case he or she is not satisfied with the handling of his or her complaint.

The BCR member and the DPCs are obliged to cooperate with the supervisory authorities in the respective country in case of requests and to respect their decision.

9.2. Cooperation with supervisory authorities

Viega Group as a whole and each BCR member undertake to cooperate with, to accept to be audited and to be inspected, including where necessary, on-site, by the competent supervisory authorities, take into account their advice, and to abide by decisions of these supervisory authorities on issues related to these BCR. Each BCR member provides the competent supervisory authority, upon request, with any information about the processing operations covered by these BCR.

9.3. Liability

Each BCR member shall be liable for its breaches of these BCR and shall also take the necessary remedial action to address such breaches.

If a non-EEA-based BCR member commits a breach of these BCR, data subjects will have the rights and remedies against Viega GmbH & Co. KG as if the violation had been caused by them in the Member State in which they are based instead of non-EEA-based BCR member. Viega GmbH & Co. KG shall ensure that a natural person whose rights have been breached is granted all rights under these BCR. This includes taking all necessary measures to stop the infringing act. Viega GmbH & Co. KG shall be liable for any material or immaterial damage suffered by the person as a result of the breach of these BCR.

Viega GmbH & Co. KG accepts responsibility arising from breaches committed by non-EEA-based BCR members, before courts or by competent authorities within the EEA.

The burden of proof for compliance with these BCR by non-EEA-based BCR members lies with Viega GmbH & Co. KG. It must prove that the company did not commit a breach of these BCR that resulted in a data subject claiming damages. The BCR member is obliged to support Viega GmbH & Co. KG in this.

9.4. Access to these BCR

Each BCR member will make the BCR available to data subjects. They will be made available via the World Wide Web on the dedicated Viega Group website.

9.5. Training of employees

Viega has a training program adopted to the specific role of the employee.

Employees who have permanent or regular access to personal data or who are involved in the collection of data or the development of tools for processing personal data shall be trained annually on the provisions of these BCR including but not limited to handling of personal data, legitimate purposes, grounds of processing, transparency, confidentiality, and processes (e.g. managing requests for access to personal data by public authorities). The training is part of the annual data protection briefing and is automatically assigned to the employees.

DPCs are trained for their role to identify processing activities, document them in the records of processing activities, answer questions of and consult their colleagues in how to implement privacy by design and understand and conduct the data protection processes. In order to maintain and update the DPCs' knowledge, regular training sessions will be conducted.

9.6. Monitoring

Viega GmbH & Co. KG conducts audits with regard to these BCR as part of the DPMS it operates in order to regularly monitor and further develop the maintenance of the appropriate level of data protection in accordance with these BCR by the BCR members. The DPM is primary accountable for conducting audits. The DPO and the Internal Audit department, or other internal or independent external auditors may conduct those audits. Conflicts of interest are ruled out by the fact that the auditor does not audit his / her own area of work. If the audits are carried out by external auditors, it must be stipulated through appropriate contracts that the confidentiality of any information is guaranteed, consulting is excluded, ethnic standards are observed and knowledge of all applicable regulations and internal company rules is available.

BCR audits are part of the Internal Audit's audit programme, which means that BCR members are audited at least once every 3 years or earlier in specific cases. Specific cases and therefore shorter audit frequencies are defined based on the risks posed by the processing activities covered by these BCR to the rights and freedoms of data subjects. These specific audits may be requested by the DPO or the DPM, who can be assisted by a team or the local DPC as appropriate. The audit programme identifies all relevant processes as well as sites to be considered.

Those BCR audits cover all aspects of the BCR including methods and action plans ensuring that corrective actions have been implemented. The scope of ad hoc audits shall be determined by the DPM or the management of the BCR members on a case-by-case basis.

The DPC, the liable BCR member, the responsible managing director of the audited company and the group board of directors are given access to the complete BCR audit report. The results of these BCR audits are made available to the competent supervisory authority upon request. Insofar as a BCR audit comes to the conclusion that remedial measures must be taken due to a BCR violation, the audited BCR member must ensure that the necessary remedial measures are implemented. Depending on the severity, the effectiveness of these measures may be checked in a follow-up audit.

10. Application and conflict of laws and regulations

10.1. General conditions

Each BCR member will adhere to and will comply with these BCR, although applicable data protection laws might be providing for a different or lower level of protection. Notwithstanding, if and to the extent applicable data protection laws stipulate stricter rules on processing, the BCR members will in addition to the BCR observe these stricter rules under applicable data protection laws.

If a BCR member has reasons to believe that the applicable legislation prevents the member from fulfilling its obligations under these BCR or it has substantial effect on the guarantees provided by these BCR, the member shall promptly inform the DPM, which in turn shall inform the Viega GmbH & Co. KG. An exception applies where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

Any legal requirement including legally binding request for disclosure of the personal data by a law enforcement authority or state security body a BCR member is subject to in a non-EEA country is likely to have a substantial adverse effect on the guarantees provided by these BCR, must be reported to the DPM. Any possibilities to appeal to such a request should be exercised. The DPM will inform the competent supervisory authority and disclose about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

If a notification is prohibited, the BCR member will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible and be able to demonstrate that it did so. If, despite having used its best efforts, the BCR member is not in a position to notify the DPM, it shall provide an annually report, providing general information on the requests it received containing the number of applications for disclosure, type of data requested, and the type of requester.

We aim to resolve any conflict between the provisions of these BCR and local laws and regulations in order to achieve an appropriate level of protection. We consult with the competent and any other supervisory authorities from the EEA in the event of legal uncertainties.

10.2. Local laws and practices affecting compliance with these BCR when transferring personal data

BCR members must use these BCR as a tool for transfers only if the requirements set out in section 7 are met and compliance with these BCR can be assessed despite applicable laws and practices. Laws and practices that respect the essence of data subjects' fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society, are not in contradiction to these BCR.

If personal data shall be transferred to a third country, an assessment must be conducted. This assessment must consider the laws and practices in the country of destination applicable to the processing of personal data, including any other requirements to disclosure of personal data or measures authorising access by public authorities that prevent the BCR member acting as a data importer fulfilling its obligations under these BCR. In assessing the laws and practices of the third country which may affect the respect of the commitments contained in these, the BCR member acting as data exporter must take due account, in particular, of 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 are transferred;
  - types of entities involved in the processing (the data importer and any further recipient of any onward transfer);
  - economic sector in which the transfer or set of transfers occur;
  - categories and format of the personal data transferred;
  - location of the processing, including storage; and
  - transmission channels used.
- The laws and practices of the country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities and those providing for access to these data during the transit between the countries involved, as well as the applicable limitations and safeguards.
- Any relevant contractual, technical, or organisational safeguards put in place to supplement the safeguards under these BCR, in particular section 6.8.4, including, measures applied during the transmission and to the processing of the personal data in the country of destination.

Where any safeguards in addition to those envisaged under these BCR shall be put in place, the BCR member liable according to section 9.3., and the DPM will be informed and involved in the assessment.

BCR members shall document such assessment appropriately, as well as the supplementary measures selected and implemented. They must make such documentation available to the competent supervisory authorities upon request.

Non-EEA based BCR members must promptly inform the data exporter if they, as data importers, encounter laws or practices that would prevent them from fulfilling its obligations under these BCR, including following a change in law or a measure (such as a disclosure request). This notification shall also be shared with the liable BCR member according to section 9.3. and the DPM, triggering reassessments. Assessments remain valid until there are changes in the laws and practices of a third country.

Upon receiving such notification, the BCR member acting as data exporter, along with the liable member according to section 9.3. and the DPM, must quickly identify additional measures (such as technical or organizational measures for security and confidentiality, as outlined in sections 6.8.5 and 6.8.6) to be adopted by the non-EEA based BCR member. This ensures the non-EEA based member's ability to meet obligations under these BCR. The same process applies if a BCR member acting as data exporter has reasons to believe that a non-EEA BCR member acting as its data importer is unable to fulfil its obligations under these BCR.

Where the BCR member acting as data exporter, along with the BCR member liable according to section 9.3. and the DPM, assesses that these BCR – even if accompanied by supplementary measures – cannot be complied with for a transfer or set of transfers, or if instructed by the supervisory authorities, the transfer or set of transfers at stake shall be suspended, 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.

Following such a suspension, the BCR member acting as data exporter must end the transfer or set of transfers if these BCR cannot be complied with and compliance with these 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, should, at the choice of the BCR member acting as data exporter, be returned to it or destroyed in their entirety.

The BCR member liable according to section 9.3. must inform the DPM who thereafter will inform all other BCR members of the assessment carried out and of its results, in order to apply the identified supplementary measures in all cases of similar type by any other BCR member. In the case where effective supplementary measures could not be put in place, the transfers at stake must be suspended or ended.

BCR members acting as data exporters will monitor, on an ongoing basis, and where appropriate in collaboration with data importers, developments in the 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 accordingly on such transfers.

11. Final provisions

11.1. Document validity

These BCR shall enter into force on 1st April 2025. They remain valid until they are replaced by an updated version.

11.2. Joining and leaving these BCR

An entity of the Viega Group can only effectively join these BCR if it can ensure compliance with these BCR. This is verified by an audit.

A BCR member that leaves these BCR shall delete or transfer the personal data processed within the scope of these BCR until the termination to a member that remains effectively bound by these BRC, unless other adequate legal instruments are used. The leaving BCR member is obliged to prove that it has fulfilled these obligations. A resignation can only be effectively executed after the proof has been presented. The same applies to any copy of the data.

11.3. Updates of these BCR

Data protection laws as well as the means, scope and purposes of data processing in general are subject to constant developments. The DPM will review these as they arise and assess whether changes to these BCR are needed. Therefore, Viega GmbH & Co. KG reserves the right to make changes and/or updates to these BCR at any time.

Where a modification to these BCR would possibly be detrimental to the level of the protection offered by these BCR or significantly affect them, it must be communicated in advance to the supervisory authorities by the DPM with a brief explanation of the reasons for the update.

Any changes to these BCR or the list of BCR members shall be reported to the competent supervisory authority once a year by the DPM. This report contains a brief explanation of the reasons for the updates. The supervisory authority is also informed once a year in instances where no changes have been made.

Changes to these BCR and to the list of BCR members shall be communicated to all BCR members without undue delay. Any changes to these BCR are binding for all BCR members.

The DPM keeps a fully updated list of the BCR members, keeps record of any updates to these BCR, and provides the necessary information to data subjects and, upon request, to competent supervisory authorities.

The currently valid version of these BCR will be published on the websites of the BCR members at least in English language. All amendments and variations of the BCR will be published on a yearly basis.