Binding Corporate Rules (BCR)

Status: Final

Scope of Applicability:

Fresenius SE & Co. KGaA and all of its affiliates according to sec. 15 et seq. of the German Stock Corporation Act except those that belong to the business segments Fresenius Kabi, Fresenius Medical Care, Fresenius Helios and Fresenius Vamed.

Fresenius Kabi Aktiengesellschaft and all those of its affiliates according to sec. 15 et seq. of the German Stock Corporation Act that belong to the business segment Fresenius Kabi.

Table of Contents

1 Definitions

In these BCR, capitalized terms shall have the following meanings:

i. "**Applicable Data Protection Laws**" means the data protection laws in a jurisdiction in effect and applicable to a Party;

ii. "**Applicable Laws**" means the entirety of laws in a jurisdiction in effect and applicable to a Party excluding Applicable Data Protection Laws; iii. "**BCR**" means this document and all its schedules;

iv. "**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;

v. **"Data Protection Advisor"** or **"DPA"** means the data protection advisor appointed within the Fresenius Group on a central level.

vi. "**Data Protection Impact Assessments**" or "**DPIA**" means a certain risk assessment in order to identify and evaluate privacy risks for Data Processing Activities, which could result in a high risk to the rights and freedoms of natural persons, for mitigating these high risks. vii. **"Data Protection Officer"** or **"DPO"** means the data protection officer appointed within the Fresenius Group according to Art. 37 GDPR, who shall not receive any instructions regarding the exercise of her/his tasks.

viii. "**Data Protection Organization**" means the data protection organization of each Party consisting of (Local) Data Protection Advisor(s) and (if legally required) the respective Data Protection Officer; ix. "**EEA**" means European Economic Area;

x. "**Employee(s)**" means any member of the management or person in an employment or quasi-employment relationship with a Party, inter alia employees, temp workers, apprentices, trainees, interns, as well as consultants and any other persons integrated into the respective Party's operational processes; xi. "**EU**" means European Union; xii. "**Framework Agreement**" means the contract between the Parties for joining the BCR.

xiii. "**Fresenius Group**" for the purposes of these BCR means Fresenius SE & Co. KGaA ("**FSE**") and all of its affiliates according to sec. 15 et seq. of the German Stock Corporation Act ("**Fresenius Entity**") except those that belong to the business segments Fresenius Kabi, Fresenius Medical Care, Fresenius Helios and Fresenius Vamed; as well as Fresenius Kabi Aktiengesellschaft ("**FK AG**") and all those of its affiliates according to sec. 15 et seq. of the German Stock Corporation Act that belong to the business segment Fresenius Kabi; xiv. "**Further Processing**" means the Processing of Personal Data by a Party located outside of the EU/EEA where the Personal Data has initially been Transferred by a Party bound by the GDPR; xv. "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

xvi. "**Individual(s)**" means an identified or identifiable natural person; 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;

xvii. **"Local Data Protection Advisor"** or **"LDPA"** means the local data protection advisor appointed within the Fresenius Group on a local level.

xviii. "**Onward Transfer**" means the Transfer of Personal Data by a Party located outside of the EU/EEA to another recipient located outside of the EU/EEA, where the Personal Data has initially been Transferred by a Party bound by the GDPR;

xix. "**Party**" or "**Parties**" means the entities of the Fresenius Group bound by the BCR and as specified in Schedule 0;

xx. "**Personal Data**" means any information relating to an identified or identifiable natural person ('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;

xxi. "**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;

xxii. "**Processor**" means an internal or external natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

xxiii. "**Special Categories of Personal Data**" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic information, biometric information for the purpose of uniquely identifying an Individual, information concerning health or information concerning an Individual's sex life or sexual orientation; xxiv. "**Supervisory Authority**" means an independent public authority which is established by a Member State pursuant to Article 51 GDPR; xxv. "**Concerned Supervisory Authority**" means a Supervisory Authority that is concerned by the Processing of Personal Data by a Party because:

- the respective Party is established on the territory of the Member State of that supervisory authority;
- the respective Party has its main establishment or its single establishment on the territory of the Member States of that supervisory authority from where the data has been transferred;
- Individuals residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the Processing; or - a complaint has been lodged with that Supervisory Authority; xxvi. "**Third Party Recipient**" means a recipient of Personal Data not being a Party to the BCR; xxvii. "**Transfer**" means any communication of Personal Data from a Controller to another Controller, to a Processor or to any another recipient.

As far as terms are not specified in this section, the document Definition BCR#16 and the definitions according to the GDPR apply.

2 Objective

The Fresenius Group operates worldwide. This includes countries where data protection laws have been and have not been enacted. To consistently regulate the way in which Personal Data is handled or processed and as part of the Fresenius Group's compliance with Applicable Data Protection Laws, the BCR participating Parties abide by an internal set of BCR for the Processing of Personal Data in order to create a uniform and adequate level of data protection across all participating Parties worldwide. The essence of BCR is to harmonise the data protection standard within the Fresenius Group on a data protection level according to EU standards. This enables an exchange of Personal Data between all Parties with an adequate level of data protection globally.

One major stakeholder for ensuring the adequate level of data protection is the group of Employees Processing Personal Data in the respective Fresenius Entity. Only if these Employees are aware about how Personal Data should be processed and what restrictions apply, an adequate standard of data protection can be achieved.

This BCR contain the essential safeguards and sets out their scope, objectives, principles and structure.

3 Scope

3.1 Territorial scope

i. The BCR **apply** in the following scenarios:

- Any Processing of Personal Data by Parties situated in the EU/EEA (including Transfers to other Parties irrespective of whether the recipients are situated in- or outside of the EU/EEA);[1]
- Any Processing of Personal Data by Parties situated outside of the EU/EEA where such Processing is rendered "in the context of the activities of an establishment" of the Fresenius Group in the EU/EEA (including Transfers to other Parties irrespective of whether the recipients are situated in- or outside of the EU/EEA); [1]
- Any Processing of Personal Data of Individuals, who are resident in the EU/EEA, by Parties situated outside of the EU/EEA, where such Processing is related to (i) the offering of goods or services to Individuals in the EU/EEA irrespective of whether a payment of the Individual is required or (ii) the monitoring of their behaviour as far as their behaviour takes place within the EU/EEA (including Transfers to other Parties irrespective of whether the recipients are situated in- or outside of the EU/EEA).[2]
- Any further Processing of Personal Data by Parties situated outside of the EU/EEA where the respectively affected Personal Data has initially been Transferred by a Party bound by the GDPR;
- Any onward Transfer of Personal Data by Parties situated outside of the EU/EEA to another recipient located outside of the EU/EEA where the respectively affected Personal Data has initially been Transferred by a Party bound by the GDPR.

ii. The BCR **do not apply** to any Processing of Personal Data by Parties situated outside of the EU/EEA where such Processing is neither

- rendered "in the context of the activities of an establishment" of Fresenius in the EU/EEA[1]
- nor related to (i) the offering of goods or services to Individuals in the EU/EEA irrespective of whether a payment of the Individual is required or (ii) the monitoring of their behaviour as far as their behaviour takes place within the EU/EEA,
- nor concerning Personal Data having been initially Transferred by a Party bound by the GDPR.

3.2 Material and personal scope

i. The 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.[3]

[1] Art. 3 para.1 GDPR

[2] Art. 3 para.2 GDPR

[3] Art. 3 para.1 GDPR

ii. The BCR also apply to those Parties which are Processing Personal Data in their capacity as (internal) Processor on behalf of another Fresenius Entity; however only to the extent they do not lead to a contradiction of a respectively concluded agreement.

iii. For the avoidance of doubt: Personal Data may[2] only be Transferred on the basis of the BCR between Parties that have duly implemented the BCR and confirmed they have successfully taken measures to establish compliance with the BCR.

iv. The BCR apply to the Processing of Personal Data by each Party listed in Schedule 1 – List of Parties bound by the BCR.

v. The BCR generally encompass the Processing operations set out in Schedule 2 - Nature of Personal Data Transferred.

3.3 Relationship between the BCR and Applicable Data Protection Laws

Each Party will adhere to and will comply with these BCR, regardless of the fact that 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 Parties will in addition to the BCR observe these stricter rules under Applicable Data Protection Laws.

3.4 Conflicts of Applicable Laws and BCR

Each Party that is bound by the GDPR shall in the course of the risk assessment in accordance with section 7 before initially Transferring Personal Data to another Party located outside of the EU/EEA assess whether the latter is capable of complying with the guarantees provided by the BCR in practice.

In case a Party has reason to believe that Applicable Laws or Applicable Data Protection Laws prevent the respective or another Party from compliance with the BCR or where this event may have a substantial impact on the standards provided by the BCR, the respective Party will immediately inform the respective Data Protection Officer in order to assess the impact and resolve the conflict, which in turn shall inform the EEA Headquarter or the EEA entity with delegate responsibilities.

Where a legal requirement such as a binding order to disclose Personal Data applicable to a Party has substantial adverse effects on the guarantees that the Fresenius Group has established by the BCR, the respective Party will report this issue specifying the data requested, the identity of the requesting body as well as the legal basis to the respective Local Data Protection Advisor who shall inform the respective Data Protection Officer, which in turn shall inform the EEA Headquarter or the EEA entity with delegate responsibilities. The Supervisory Authority in Hesse, Germany, will be informed by the respective Data Protection Officer. All information will be done without undue delay.

In case such notification is prohibited by Applicable Laws, the Party will use best efforts to receive permission to inform the respective Data Protection Officer and subsequently the Supervisory Authority in Hesse, Germany as soon as possible with information to the greatest possible extent.

Where a Party is not permitted to provide specific information on a request, the Party will provide general information on requests received on an annual basis to the respective Data Protection Officer with relevant information to the greatest possible extent (detailing in particular the number of received and followed disclosure orders, requesting bodies, affected categories of Individuals and types of Personal Data) to enable to inform the Supervisory Authority in Hesse, Germany.

[2] 4 Artt. 46 para. 2 lit. b, 47 GDPR

In any case, Transfers of Personal Data by a Party to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

4 Binding nature of the BCR / Third-party beneficiary rights

The BCR are binding for each Party and its Employees. Individuals are third party beneficiaries and can derivate rights from the BCR. Each Party and each of its Employees is obliged to respect the principles and obligations laid down in the BCR.

The binding nature of the BCR encompasses:

i. *Binding nature for Parties* – The Fresenius Group has introduced the BCR within the Parties and set up a mechanism to make the BCR binding upon any Party listed in Schedule 1 – List of Parties bound by the BCR. Each Fresenius Entity has contractually bound itself to adhere to the principles of the BCR by signing the Framework Agreement with all participating Parties. Where this is necessary for the BCR to be effective, each Party is obliged to implement all additional requirements to make the BCR binding as contractually required. ii. *Binding nature for Employees* – Employees are obliged to respect the principles laid down in the 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 Party is obliged to implement all additional requirements to make the BCR binding as contractually required.

iii. *Binding nature towards Individuals* (third party beneficiary rights) – All Parties commit to granting Individuals third party beneficiary rights under the BCR in respect of the Processing of their Personal Data. Accordingly, it is expressly acknowledged and accepted by each Party that Individuals will be entitled to enforce the provisions of clauses 3.3, 3.4, 4, 6.1–6.8, 9.1-9.7 and 10.1-10.4 of this BCR in respect of the Processing of their Personal Data and as further stipulated under section 10.

5 Data Protection Organization

Fresenius Group established an internal data protection organization, and assigned roles and responsibilities within the Parties in order to achieve an adequate governance and support framework to ensure lawful Processing of Personal Data. Fresenius Group will designate a DPO where required and maintain the data protection organization to continue adequate governance and support for each Party as follows:

- The Data Protection Officer (DPO) monitors, assesses and audits compliance with the BCR and Applicable Data Protection Laws and data protection policies and procedures. The DPO informs and advises the respective Party and Employees of their obligations under the BCR and Applicable Data Protection Laws, provides advice where requested and in case of Data Protection Impact Assessments, investigates violations and monitors remediation of such violations, proposes improvements to the data protection management system and cooperates with and acts as primary contact point for Supervisory Authorities. The DPO is in charge for the scope outlined in its appointment and reports directly to the highest management. In this role the DPO acts independently.
- The Data Protection Advisor (DPA) provides supporting and consulting task within the Data Protection Organisation, builds, deploys and maintains the data protection management system in order to enable lawful Personal Data Processing and adherence to the BCR and Applicable Data Protection Laws. Furthermore, the DPA reviews Personal Data Processing concepts relevant to the Fresenius Group, runs data protection risk assessments, advises on data processing agreements, supports business process owner with recording Data Processing

Activities, consults on Data Protection Impact Assessments, prepares responses to data subject inquiries and enables the LDPAs to provide competent advice.

Where necessary the DPA supports the DPO on request in its monitoring function and contact with Supervisory Authorities e.g., due to language issues.

- The Local Data Protection Advisor (LDPA) provides advice and support to the Business or Process Owner for all activities of the respective local Fresenius Entity or on a specific topic, supports in language issues, performs risk assessments relevant to the local entity or topic

  and reviews relevant data processing concepts and agreements, supports business process owner with maintenance of the registration of Data Processing Activities and documentation of relevant data protection measures.

  Where necessary the LDPA supports the DPA and DPO.

  LDPA are merely assigned within FK AG.

The Data Protection Officer of FSE and all of its affiliates according to sec. 15 et seq. of the German Stock Corporation Act except those that belong to the business segments Fresenius Kabi, Fresenius Medical Care, Fresenius Helios and Fresenius Vamed can be contacted as follows:

Data Protection Officer Fresenius SE & KGaA

Fresenius SE & Co. KGaA
Else-Kröner-Str. 1
61352 Bad Homburg v.d.H. Germany
dataprotectionofficer@fresenius.com

The Data Protection Officer of FK AG all those of its affiliates located in the EU/EEA according to sec. 15 et seq. of the German Stock Corporation Act that belong to the business segment Fresenius Kabi can be contacted as follows:

Data Protection Officer Fresenius Kabi

Fresenius Kabi AG
Else-Kröner-Str. 1
61352 Bad Homburg v.d.H.
Germany dataprotectionofficer@fresenius-kabi.com

6 Data Protection Principles under BCR

Parties respect the importance of Individual's privacy. When Personal Data held by Parties is Processed, the fundamental rights and freedoms of Individuals, in particular their right to the protection of Personal Data, must be respected.

Within the scope of this BCR, each Party will comply with the following principles when Processing Personal Data:

6.1 Lawfulness

Each Party will only process Personal Data in a lawful manner. The specific legal basis of the respective Data Processing Activity shall be documented accordingly. Party will only Process Personal Data on the following legal grounds[3]:

[3] Art. 6 GDPR

i. On the basis of the Individual's consent, meaning the freely given, specific, informed and unambiguous indication by which the Individual signifies agreement to the Processing of his or her Personal Data for one or more specified purposes;

ii. for the performance of a contract to which the Individual is a party or in order to take steps at the request of the Individual prior to entering into a contract;

iii. for compliance with the Fresenius Group's statutory or legal obligations, for example those relating to taxation, medical device or pharmacovigilance duties;

iv. where the Processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the respective Party;

v. in order to protect the vital interests of an Individual or of another natural person; vi. for the purpose of a legitimate interest of the respective Party or another third party unless the Individual has an overriding interest in his or her Personal Data not being processed (see 9.6).

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 Supervisory Authority or when the Processing is authorized by Applicable Data Protection Law providing for appropriate safeguards for the rights and freedoms of Individuals. Section 3.4 remains unaffected.

Applicable Data Protection Laws and Applicable Laws may stipulate additional or divergent provisions with regard to the Processing of Personal Data of Employees. In such case, the Parties will process Personal Data of Employees in accordance with such provisions. Sections 3.3 and 3.4 remain unaffected.

Party will only process Special Categories of Personal Data on the following legal grounds[4]:

i. on the basis of the Individuals' explicit consent to the Processing of those personal data for one or more specified purposes; ii. if necessary for employment or social security purposes;

iii. in order to protect the vital interests of an Individual or of another natural person where the Individual is physically or legally incapable of giving consent; iv. if Personal Data was manifestly made public by the Individual;

v. if necessary for the establishment, exercise or defence of legal claims;

vi. if necessary for reasons of substantial public interest as far as proportionate to the aim pursued, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard the fundamental rights and the interests of the Individuals;

vii. if necessary for purposes of preventive or occupational medicine, for the assessment of the working capacity of Employees, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;

viii. if necessary for reasons of public interest in the area of (cross border) public health, such as ensuring high standards of quality and safety of health care and of medicinal products or medical devices, securing the rights of the Individuals, in particular professional secrecy; or

ix. if necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, provided that the Processing respects the essence of the right to data protection and takes suitable and specific measures to safeguard the fundamental rights and the interests and principles of the Individuals laid down in this BCR.

6.2 Transparency and Fairness

Each Party will process Personal Data fairly and in a transparent manner[5] which means that Individual will generally be adequately informed in advance[6] on the Processing of their Personal Data, and be provided with information on their Data Subjects' Rights as per Section 9 below as well as any other rights conferred to them by Applicable Data Protection Laws in relation to their Personal Data (see section. 9 below).

[4] Art. 9 GDPR

[5] Art 5, Para 1, lit. (a) GDPR

[6] Art. 13 & 14 GDPR

If the Personal Data is not obtained from the Individual, the information will be provided:

i. within a reasonable period after obtaining the Personal Data, but latest within one month; having regard to the specific circumstances in which the Personal Data are processed;

ii. if the Personal Data are to be used for communication with the Individual, at the latest at the time of the first communication to that Individual; or

iii. if a disclosure to another recipient is envisaged, at the latest when the Personal Data are first disclosed.

Any information provided to Individuals or any communication with an Individual that relates to the Processing of their Personal Data will be concise, transparent, comprehensive and in an easily accessible form, using clear and plain language.

6.2.1 Obligatory Information

Such transparent information to the Individual will include the following:

i. the identity and the contact details of the Party and, where applicable, of the Fresenius Entity's representative; ii. the contact details of the Data Protection Officer, where appointed;

iii. the purposes of Processing of the Personal Data as well as the legal basis for the Processing; iv. if Processing is based on legitimate interest, the legitimate interests pursued by the Party or a third party;

v. the recipients or categories of recipients of the Personal Data (if any); vi. any Transfer of Personal Data to a country outside the EU/EEA or international organization, the legal basis on which such Transfer is based including 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.

6.2.2 Additional Information to be provided

In order to ensure fair and transparent Processing the following additional information will be provided:

i. the period for which the Personal Data will be stored;

ii. the rights of Individuals as listed in section 9 of this Binding Corporate Rules;

iii. where the Processing is based on consent, the existence of the right to withdraw consent at any time which will only have effect for the future Processing of Personal Data;

iv. the right to lodge a complaint with a Supervisory Authority;

v. any existence of automated decision-making, including profiling, and meaningful information about the logic involved as well as the significance and the envisaged consequences of such processing.

vi. 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 Individual is obliged to provide the Personal Data and of the possible consequences if the Personal Data is not provided;

6.2.3 Additional information to be provided in case data is collected from a third party.

In case Personal data is collected from a third party different to the Individual, the Party will provide additionally information on:

i. the categories of Personal Data being Processed; and ii.

the source of the Personal Data.

6.3 Purpose Limitation

Any Party will process Personal Data only for the specified purposes for which the Personal Data are collected. Any Party will not process Personal Data for purposes that are incompatible with the initial 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 Individual such as the consent of the respectively affected Individuals, limiting access to the Personal Data, additional confidentiality and security controls, provision of information to the Individual.

Generally permitted purposes for further Processing, which are deemed compatible with the original purpose are:

i. archiving; ii. 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:

i. any link between the purposes for which the Personal Data have been collected and the purposes of the intended further processing;

ii. the context in which the personal data have been collected, in particular regarding the relationship between Individuals and the respective Party;

iii. the nature of the Personal Data, in particular whether Special Categories of Personal Data are Processed, pursuant to Article 9 GDPR, or whether Personal Data related to criminal convictions and offences are Processed, pursuant to Article 10 GDPR;

iv. the possible consequences of the intended further Processing for Individuals;

v. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

The (Local) Data Privacy Advisor will be able to provide guidance as to if and when such change is permitted.

In case of a permitted change of purpose, Individuals must be informed of any such changes in accordance with section 6.2 before the Personal Data is processed for that other purpose.

6.4 Data Minimisation

Any Party will collect and Process Personal Data only to the extent necessary for the business purpose and about which the data subject is informed (initial purpose) or those that are compatible with these initial purposes in accordance with section 6.3. Any Party will not collect or Process Personal Data that is either excessive or not relevant for the purpose for which the Personal Data is needed.

6.5 Accuracy

Personal Data will be kept by Fresenius Group accurate and up-to-date. Each Party will implement procedures to ensure that inaccurate data is deleted, corrected or updated throughout the respective lifecycle without delay.

6.6 Storage Limitation

Each Party will keep Personal Data no longer as is necessary for the purpose the Personal Data is processed for, unless the Personal Data are to be retained by law. If Personal Data must be retained for other reasons than its original purpose (e.g. because applicable 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 Party anymore, the Personal Data will be anonymised or securely deleted.

6.7 Security, Integrity and Confidentiality

6.7.1 Technical and Organizational Security Measures

Each Party will take appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed. Each Party will consider in particular the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for the rights and freedoms for Individuals when implementing such technical and organizational measures considering the confidentiality, integrity and availability of stored Personal Data by installing and maintaining data Processing systems and services set up to remain resilient against cybersecurity attacks and IT security threats, including inter alia as appropriate:

i. the pseudonymisation and encryption of Personal Data;

ii. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; iii. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

iv. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

6.7.2 Notification of Personal Data Breaches

Each Party commits to notify any breach of security leading to any accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure of or access to Personal Data to the Data Protection Organization of FSE and FK AG which in turn shall inform the EEA Headquarter. In addition, the following notification obligations exist in case of such a personal data breach:

i. any Party, subject to the GDPR and operating as Controller shall notify any personal data breach that is likely to result in a risk for the affected Individuals to the Supervisory Authority without undue delay and, where feasible, not later than seventy-two (72) hours after having become aware of the personal data breach;

ii. any other Party, operating as Controller shall notify any personal data breach that is likely to result in a risk for the affected Individuals to the Concerned Supervisory Authority without undue delay and, where feasible, not later than seventy-two (72) hours after having become aware of the personal data breach;

iii. any Party, operating as Processor for another Party shall notify any personal data breach to the respective Party operating as Controller and the relevant LDPA.

iv. where a personal data breach is likely to result in a high risk to the rights and freedoms of the affected Individuals, the respective Party operating as Controller shall communicate the personal data breach to the affected Individuals without undue delay.

Each Party 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 Data Protection Organization of FSE and FK AG make such documentation available to Supervisory Authorities.

6.8 Accountability

Each Party will adhere to the principles set out above and will be able to demonstrate compliance with the BCR and in this respect, will create and maintain appropriate documentation, including:

i. Maintaining Records of Processing Activities respectively stating:

- the name and contact details of the Controller and, where applicable, the joint controller, the Controller's representative and the Data Protection Officer;
- the purposes of the Processing;
- a description of the categories of Individuals 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 outside of the EU or an international organization, including suitable safeguards as defined in section 6.8.2;
- where possible, the envisaged time limits for removing of the different categories of Personal Data;
- where possible, a general description of the technical and organisational security measures referred to in section 6.7.

This record should be maintained in writing, including in electronic form and should be made available to Supervisory Authorities on request.

ii. Implementing appropriate technical and organizational measures which are designed to implement data protection principles and to facilitate compliance with the requirements established by the BCR in practice (data protection by design and by default).

iii. Carrying out Data Protection Impact Assessments as set forth in section 8.

6.8.1 Engagement of Processors

Each Party will only engage Processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that Processing will meet the requirements of the BCR and Applicable Data Protection Laws (in particular the GDPR) and ensure the protection of the rights of the Individuals.

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:

i. that the Processor must solely Process Personal Data in accordance with the received instructions from the data controller;

ii. that the Processor must maintain appropriate technical and organizational measures to protect Personal Data;

iii. that the Processor ensures that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

iv. that the Processor must delete or return all Personal Data after the end of the provision of services relating to Processing and deletes existing copies;

v. that the Processor may solely engage sub-processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that Processing will meet the requirements of the BCR and Applicable Data Protection Laws on basis of written contractual means imposing the same level of data protection obligations on the sub-processors as set out between the Party and Processor;

vi. that the Processor will support the respective Party in fulfilling its obligations to respond to requests of Individuals;

vii. that the Processor makes available all information necessary to demonstrate compliance with this section and allow for and contribute to audits, including inspections by the respective Party or another agreed upon auditor; viii. that the Processor will assist the respective Party in ensuring compliance with the obligations as mentioned in sections 6.7 and 7.

6.8.2 (Onward) Transfers of Personal Data

The Parties will implement measures to adequately safeguard Transfers of Personal Data to Third Party Recipients situated outside of the EEA in compliance with these BCR.

Personal Data may solely be Transferred to a Third Party Recipient outside of the EEA in case at least one of the following conditions is met:

i. the Third Party Recipient is located in a country which has been recognized by the European Commission as offering an adequate level of protection for Personal Data (so called "White List" countries) and – as far as applicable – the Third Party Recipient fulfils all additional requirements under the applicable adequacy; or

ii. if the Third Party Recipient has provided appropriate safeguards and on condition that enforceable Individual rights and effective legal remedies are available to the Individuals; e.g. by virtue of standard contractual clauses adopted by the EU-Commission; or

In derogation of the aforementioned alternatives, Personal Data may be also be Transferred in case one of the following exceptions applies:

i. the Individual has given her/his explicit consent for the Transfer of her/his Personal Data after having been informed of the possible risks of such transfers; or

ii. the Transfer of Personal Data is necessary (i) to perform a contract with the Individual or implement pre-contractual measures taken at the Individual's request; or (ii) to perform or conclude a contract concluded in the interest of the Individual between the Controller and another natural or legal person; or

iii. the Transfer of Personal Data is necessary (i) to protect the Individual's vital interests or of other persons (i.e. in case of a life or death situation), where the Individual is physically or legally incapable of giving consent, or (ii) to allow Fresenius to establish, exercise or defend a legal claim, or (iii) for important reasons of public interest; or

iv. the Transfer is made from a register which according to EU or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or Member State law for consultation are fulfilled in the particular case.

If none of the above conditions is met, and the Transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests and these are not overridden by the interests or rights and freedoms of the data subject, the sending Party will assess the circumstances surrounding the data Transfer and provide suitable safeguards with regard to the protection of Personal Data and inform the Concerned Supervisory Authority of the Transfer.

For the avoidance of doubt, the aforementioned conditions also apply for any Onward Transfer of Personal Data by a Party situated outside of the EU/EEA to a Third Party Recipient located outside of the EU/EEA where the respectively affected Personal Data has initially been Transferred by a Party located in the EU/EEA.

7 Data Protection Risk Assessment

Each Party will carry out a Data Protection Risk Assessment for any Data Processing Activity related to Personal Data. The Data Protection Risk Assessment is a formal process to assess the impact of any Data Processing Activity on the rights and freedom of the respective concerned Individuals (Privacy Risks). The Risk Assessment is conducted as a detailed analysis of a Data Processing Activity and serves the purpose of identifying:

i. Privacy Risks for the Individuals resulting from the Data Processing Activity;

ii. applicable requirements stemming from the BCR and Applicable Data Protection Laws; and

iii. suitable measures to fulfil these requirements and mitigate the identified Privacy Risks.

In particular, each Party shall before Transferring Personal Data to another Party located outside of the EU/EEA assess whether the latter is capable of complying with the guarantees provided by the BCR in practice taking into consideration the context and purpose of the data transfer, the possible interference created by Applicable Laws or Applicable Data Protection Laws in the third country concerned with the fundamental rights of the Individuals. If this should not be the case, the Parties shall assess whether they can provide supplementary technical, organizational or contractual measures/controls to ensure an essentially equivalent level of protection as provided in the EU. If such measures could not be provided the Party does not carry out the Transfer. If the Party is already Transferring Personal Data, the transfer shall be suspended or end. Personal Data already transferred, or copies thereof should be returned to the sending Party or destroyed in their entirety by the recipient. Any assessments rendered under this paragraph shall be reviewed on a regular basis.

The Risk Assessment consists of the following main steps:

iv. Pre-Assessment

The Pre-Assessment determines the inherent Privacy Risks resulting from a Data Processing Activity and qualifies them as high, medium or low. The results of the Pre-Assessment determine the further steps of the Risk Assessment.

v. Controls Assessment

Within the Controls Assessment the measures/controls implemented or, necessary to be implemented, are determined and documented according to three maturity levels to mitigate the inherent risks defined by the pre-assessment and where applicable because of a high risk, defined by the DPIA, and to fulfil the requirements of the BCR and Applicable Data Protection Laws.

vi. Assess Adequacy of Data Protection Controls

The adequacy of the implemented or to be implemented technical, organizational or contractual measures is assessed to determine the residual Privacy Risks.

vii. Risk Reporting

The identified control gaps and potential residual risks are reported and documented. The gaps and risks must be remediated, and the mitigating technical and organizational measures must be implemented before the Data Processing Activity is started.

If the Pre-Assessment results in a high Privacy Risk a Data Processing Impact Assessment (DPIA) has to be conducted additionally by the respective (Local) Data Privacy Advisor and approved by the respective Data Protection Officer.

8 Data Protection Impact Assessments[7]

Each Party will carry out a Data Protection Impact Assessment (DPIA) where the Processing of Personal Data is likely to result in a high risk to the rights and freedoms of Individuals prior to Processing. The advice of the respective Data Protection Officer will be sought.

In order to assess whether a DPIA is necessary the Party will take into account the type of Processing, use of new technologies as well as the nature, scope, context and purposes of the Processing. Where a DPIA identifies a high risk of specific Data Processing Activity, the responsible Party will implement adequate measures to mitigate such risks prior to the start of

[7] Art.35 GDPR

the Processing. Where a DPIA indicates that the Processing would still result in a high risk taking into account the measures taken to mitigate the risk, the Concerned Supervisory Authority, prior to Processing, should be consulted.

DPIA will in particular be required in the case of:

i. systematic, extensive and automated Processing of Personal Data, including profiling and where decisions that have significant effects on Individuals, or

ii. a large scale of Processing Special Categories of Personal Data or relating to criminal convictions and offences.

9 Individuals' Rights[8]

Each Party will enable Individuals to exercise the following rights.

Each Party will inform recipients if and to the extent an Individual requests rectification, deletion or restriction of Personal Data, unless this proves impossible or involves disproportionate effort. Parties will inform the Individual about those recipients on the Individual's request. Any request that a Party may receive from an Individual in relation to her/his aforementioned rights will be handled in accordance with the BCR complaint handling as described in section 10.2.

9.1 Right to access Personal Data

The Individual has the right to request to access/receive information about their Personal Data, the purpose of Processing, the categories of Personal Data concerned, the recipients of Personal Data, storage periods for Personal Data or its criteria, the existence of the right to request rectification or erasure of Personal Data or restriction of Processing of Personal Data concerning the Individual or to object to such Processing, the right to lodge a complaint with a Supervisory Authority and the source of the Personal Data where the Personal Data are not collected from the data subject, any existence of automated decision-making, including profiling, any Transfer to a country outside the EU/EEA and obtaining a copy of the Personal Data undergoing Processing (see also sec. 6.2).

9.2 Right to rectify Personal Data

The Individual has the right to request rectification of inaccurate or incomplete Personal Data relating to him or her processed by a Party and to have incomplete Personal Data completed.

9.3 Right to erase Personal Data

The Individual has the right to request deletion of his or her Personal Data processed by a Party, provided that and to the extent either of the following conditions is met: (i) the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise Processed, (ii) the Individual withdraws consent on which the Processing is based and where there is no other legal ground for the Processing, (iii) the Individual objects to the Processing pursuant and there are no overriding legitimate grounds for the Processing, or the Individual objects to the Processing for the purposes of direct marketing, which includes profiling to the extent that it is related to such direct marketing, (iv) the Personal Data have been unlawfully Processed or (v) the Personal Data have to be erased for compliance with a legal obligation in Applicable law to which the controller is subject. Existing data retention obligations and/or conflicting interests must be observed; section 3.4 applies.

[8] Chapter III GDPR

9.4 Right to restrict Processing of Personal Data

The Individual has the right to request the restriction of Processing of his or her Personal Data if either (i) the accuracy of the Personal Data is contested by the Individual or the Individual has objected to Processing (see below section 9.6), for a period enabling the respective Party to verify the accuracy of the Personal Data or whether the legitimate grounds of the respective Party override those of the Individual; or (ii) the Processing is unlawful, respectively no longer required for the respectively pursued purposes but the Individual opposes the erasure of the Personal Data and requests the restriction of their use instead (e.g. if the Personal Data is required for the establishment, exercise or defence of legal claims).

9.5 Right to receive Personal Data in a portable format and transmit Personal Data

Where Personal Data have been provided by the Individual and the Processing is based on the Individual's consent or on a contract with the Individual and the Processing is carried out by automated means, the Individual 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 Individual to use similar services from another Controller.

9.6 Right to object to the Processing of Personal Data

The Individual has the right to object on grounds relating to his or her particular situation to the Processing of their Personal Data based on the Parties' or a third parties' legitimate interests or public interests (this right does not apply if a legal provision requires the Personal Data to be processed). The Processing will cease unless the respective Party demonstrates compelling legitimate grounds for the Processing which override the interests, rights and freedoms of the Individual or for the establishment, exercise or defence of legal claims.

Further, the Individual has the right to object to the Processing of Personal Data relating to him or her for the purposes of direct marketing, which includes profiling to the extent that it is related to such direct marketing.

9.7 Right not to be subject to automated decision making

Individuals will also have the right not to be subject to a decision based solely on automated Processing, including profiling, by a Party which could lead to legal or similar significant effects on the Individual, unless that decision:

i. is necessary for entering into or performance of a contract between the Individual and the respective Party, or is based on the Individual's explicit consent, provided that the respective Party has implemented suitable measures to safeguard the Individual's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of Party, to express his or her point of view and to contest the decision; or

ii. is authorized by Applicable Law to which the respective Party is subjected to and which also lays down suitable measures to safeguard the Individual 's rights and freedoms and legitimate interests. Section 3.4 remains unaffected.

To this end, Special Categories of Personal Data may solely be Processed either if the Individual has given her/his explicit consent, or it is authorized by Applicable Law to which the respective Party is subjected to which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Individual.

10 Compliance with BCR

10.1 Access to BCR

Each Party will make the complete BCR available, especially those sections that confer rights on Individuals, specifically section 3.3, 3.4, 4, 6.1 – 6.8, 9.1- 9.7 and 10.1-10.4 of the BCR, available for Individuals externally via the World Wide Web on the dedicated Fresenius Group website. The

complete BCR will also be made available internally via Fresenius Group's intranet websites. Individuals can also access the complete BCR versions approved for publication by contacting the respective Data Protection Officer or any member of the Data Protection Organization.

10.2 BCR complaint handling

Each Individual is entitled to claim violation of the BCR, address its Individual rights as set out in sec. 9 of this BCR, enforce any other right of the BCR, or issue any other request to the Data Protection Organization. Fresenius will implement procedures to ensure that such complaint is dealt with.

Complaints means any report claiming a potential violation of the BCR, Applicable Data Protection Laws, orders by Supervisory Authorities, internal policies and guidelines or voluntary selfcommitments relating to data protection. In contrast, data subjects' rights requests are all requests by an Individual referring to the rights according to section 9 of this BCR in accordance to a data subject request handling procedure.

Any such complaints can be submitted by multiple channels for raising a complaint. A request can be submitted e.g. via phone or in writing e.g. by email or letter or orally by approaching the respective Data Protection Officer, the respective (Local) Data Protection Advisor or the Compliance Hotline. The respective communication channels are published on the Fresenius World Wide Web and internal websites of the Fresenius Group providing any necessary information (https://www.fresenius.com/compliance – reports on potential compliance cases or https://www.fresenius-kabi.com/responsibilities/compliance).

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 Fresenius or any Employee will be rejected. In such an event, the Individual 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 Party 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 Individual will be notified in writing that adequate action(s) to address the complaint will be or have been initiated. In any case, the Individual 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 10.3 in case he or she is not satisfied with the handling of his or her complaint.

For data subject requests the Data Protection Officer with support of the (Local) Data Protection Advisor will endeavour, wherever possible, to issue a substantial response to the Individual within one (1) calendar month from receipt of the complaint. Where it is not possible to provide a substantial response within one (1) calendar month, for example due to the nature of the complaint, the Individual will be notified by the respective Data Protection Officer with support of the respective (Local) Data Protection Advisor, providing an estimate as to when they may expect to receive a substantial response. A substantial response will be provided not later than three (3) months after receipt of a complaint.

Additionally, the contact details of the Data Protection Officer and other members of the Data Protection Organization are provided above in section. 5 of this Binding Corporate Rules.

The Data Protection Organization documents Individuals´ actions according to this section 10.2.

10.3 Liability and Enforcement

Individuals who are affected by or have suffered damages as a result of the Processing of their respective Personal Data, that is unlawful or contrary to the enforceable parts of the BCR as set forth in section 4, either by a Party or an engaged Processor or sub-processor, are entitled to bring actions or proceedings in order to enforce these parts of the BCR and if applicable to receive compensation before a competent court, either in the country where a Party is established or in Bad Homburg, Germany where FSE and FK AG are established, or where the respective Individual has his or her habitual residence, and before Supervisory Authorities in particular in the country

of the Individuals' habitual residence, place of work or place of the alleged infringement e.g., by raising a complaint.

In case of proven violations of the enforceable parts of the BCRs as set forth in section 4 by Parties established outside the EU/EEA, FSE accepts responsibility and liability for any damages caused by such violation of the BCR, and agrees to take any appropriate action to remedy the acts of Parties established outside the EU/EEA and to pay compensation for any material or non-material damage occurring to an Individual from any such violation. Prior to paying any compensation or making any statements towards the data subject, FSE will give the concerned Party prompt notice of the demand to allow the concerned Party to seek a protective order or other appropriate remedy. FSE is entitled by itself to seek protective order or other appropriate remedy against the alleged violation.

Where Individuals can demonstrate that they have suffered damages and coherently state facts which show it is likely that the alleged violations, respectively that the damage has occurred because of the alleged violation of the BCR, FSE has to prove vis-á-vis the Individual that the Party causing the damage was not responsible for the violation of the BCR giving rise to those damages or that no such violation took place. The Party, who caused the damage, shall provide reasonable assistance to FSE to respond to such complaints or requests in a timely manner.

Any Party located outside of the EU/EEA will adhere to any request or order by a Supervisory Authority that would be binding on the Party as if the Party was established in the EU/EEA.

10.4 Cooperation with Supervisory Authorities

Each Party is required to (i) cooperate with the Concerned Supervisory Authorities, (ii) comply with the advice concerning any issue on the interpretation of these BCR (iii) accept being audited by the Concerned Supervisory Authorities. On request of a Concerned Supervisory Authority, the respective Data Protection Officer will provide a copy of the applicable audit report created under the audit program as described in sec. 10.6.

10.5 Training

Each Party will enrol and oblige their Employees involved in the Processing of Personal Data or in the development of tools used to Process Personal Data to participate in a training on the BCR and Applicable Data Protection Laws and to regularly repeat such training. General training is at least bi-annually provided to all relevant Employees. Furthermore, role specific training (such as dedicated information and coaching sessions or workshops) is provided taking into account the specific needs of certain roles/persons, e.g. the members of the Data Protection Organization of FSE and FK AG.

Training is mandatory for the relevant Employees. Once being invited by email to attend a training, the Employee is given a predetermined time for its completion. Employees that have not attended a training at a given time will receive a reminder. Additionally, the Employee's supervisor receives a reminder notification that will be resent on a monthly basis until the training has been completed. An Employee who does not attend a respective training after two reminders may be subject to (disciplinary) consequences in accordance with applicable employment law.

Training will in most cases be provided via an e-Learning platform. Generally, trainings end with a validation to help solidify the understanding of the contents e.g. by using a multiple choice or free text field test.

10.6 Auditing

The Parties implement and commit to maintain an audit program covering data protection related areas at a Party, in particular all aspects covered by the BCR. All Parties will commit to be regularly audited to evaluate and test compliance with the BCR and implement adequate and sufficient mechanisms to remedy non-compliance of a Party with the BCR. There will be planned audits which are supplemented by ad hoc audits in case required by the Data Protection Organization or the management of the Parties.

Planned audits shall *inter alia* cover the following areas: (i) Data protection governance (e.g. the extent to which data protection policies and procedures to comply with the BCR are in place and in operation etc.), (ii) security of Personal Data (e.g. the technical and organizational measures in place to ensure adequate security over Personal Data Processed etc.), (iii) Training and awareness (e.g. provision and attendance of data protection training etc.), (iv) Individuals' and Supervisory Authorities' requests (e.g. procedures in operation for responding to Individuals' requests as well as communication with Supervisory Authorities etc.), (v) Data Transfers: Compliance with the BCR in particular based on potential interference by Applicable Law etc.

The Frequency and sequence of planned audits will be determined yearly in an audit plan based on the risks associated with the relevant Transfers, taking into consideration *inter alia* the following aspects: (i) volume of Personal Data, (ii) sensitivity of Personal Data (including whether Special Categories of Personal Data is affected), (iii) types of Individuals, (iv) the criticality for internal operations as well as (v) potential impact to Individual in particular on basis of carried out Data Protection Impact Assessments (see section 8). The number of Parties audited within a year shall however not fall below 5.

The scope of *ad hoc* audits shall be determined by the Data Protection Organization or the management of the Parties on a case-by-case basis.

Outcome of each audit will be an audit report which will be issued officially to all Auditee's, the relevant board or senior management of the controlling undertaking, the LDPA, the respective Data Protection Officer, and the Chief Compliance Officer of the Parties. The Data Protection Organization will follow up on any conducted audit to assess whether proposed corrective actions have been appropriately implemented and document any outcomes in the audit report. Each Party will make audit reports available to Supervisory Authorities upon request.

Audits will be executed either by the Data Protection Officers, by the Internal Audit department of Fresenius or external auditors, in collaboration with the Data Protection Officers of the respective sector taking into account any conflicts of interest by ruling out that the auditor is auditing his own area of work.

10.7 Update of BCR

Data protection laws as well as the means, scope and purposes of Data Processing in general are subject to constant developments. Parties will review these as they arise and assess whether changes to the BCR are needed. Fresenius therefore reserves the right to amend the BCR including, without limitation, adding new Parties to the BCR or removing Parties from the BCR.

Any changes to the BCR that will significantly affect the level of data protection offered by the BCR or the BCR themselves, including administrative changes if they impact the BCR, will promptly be reported to each Party and to the Supervisory Authority in Hesse, Germany (BCR Lead). Any other non-substantive amendments to the BCR will be reported to the Supervisory Authority in Hesse, Germany on an annual basis including a brief explanation of reasons justifying the amendment; Parties will be notified of such changes as soon as practicable, in any case within two (2) months prior to the amendment or variation of the BCR coming into effect. All amendments and variations of the BCR will be published on a yearly basis. For the avoidance of doubt: The Supervisory Authority in Hesse, Germany is at liberty to share any of these reports with other Supervisory Authorities.

The Data Protection Officers of FSE and FK AG in collaboration keep an up to date register that includes (i) the details of all Parties bound to the BCR and (ii) a record of all updates to the BCR. They will also enable the Supervisory Authorities or Individuals to access the information of the register on request.

11 Exit Management

In case a Party ceases to adhere to the BCR (i.e. via termination of the respective intra-groupagreement), such Party will either (i) promptly and respectively return all Personal Data to any Parties having Transferred Personal Data to the leaving Party during the term of the latter's participation in the BCR or (ii), in compliance with local data retention rules, destroy all such Personal Data and certify in writing to the Transferring Parties that such Personal Data has been destroyed, or (iii) will otherwise provide for sufficient safeguards with regard to such Personal Data in the meaning of Artt. 44 et seq GDPR (e.g. by concluding standard contractual clauses adopted by the EU-Commission). If the leaving Party cannot provide such sufficient safeguards, the leaving Party may only continue Processing such Personal Data for the future and to the extent a derogation pursuant to Art. 49 GDPR applies (i.e. merely for such purposes covered by the respectively applicable derogation).

12 References

n/a

13 Document Change History

Version	Reason for Change & Change Description	Author	Date
1	Final FDPB	DPO	15.07.2022

Schedule 1: List of Parties bound by the BCR

No.	Name and Description of Fresenius Entity	Country of Establishment
1	Fresenius Kabi S.A	Argentina
2	Nutri Home S.A	Argentina
3	Fresenius Kabi Australia Pty Ltd.	Australia
4	Fresenius Kabi Austria GmbH	Austria
5	Fresenius Kabi N.V.	Belgium
6	Gan Rio Apoio Nutricional - Ganutre Ltda.	Brazil
7	Fresenius Kabi Brasil Ltda.	Brazil
8	Fresenius HemoCare Brasil Ltda.	Brazil
9	Fresenius Kabi Bulgaria EOOD	Bulgaria
10	Fresenius Kabi Canada Ltd.	Canada
11	Calea Ltd.	Canada
12	Calea Vancouver Inc.	Canada
13	Calea Pharmacy Ltd.	Canada
14	Fenwal International Inc., Cayman Islands	Grand Cayman

15	Fenwal International Inc., Domenican Republic branch	Dominican Republic
16	Fenwal International Inc., Puerto Rico branch	Puerto Rico
17	Fresenius Kabi Chile Ltda.	Chile
18	Recetario Magistral Endovenoso S. A.	Chile
19	Laboratorio Sanderson S. A.	Chile
20	Beijing Fresenius Kabi Pharmaceutical Co., Ltd.	China
21	Fresenius Kabi (Beijing) Pharmaceutical Distribution Co. Ltd.	China
22	Fresenius Kabi (China) Co. Ltd.	China
23	Fresenius Kabi (Guangzhou) Co. Ltd.	China
24	Fresenius Kabi (Nanchang) Co., Ltd.	China
25	Fresenius Kabi Sino-Swed Pharmaceutical Corp. Ltd.	China
26	Fresenius Kabi Colombia S.A.S.	Colombia
27	Fresenius Kabi d.o.o.	Croatia
28	Fresenius Kabi Horatev CZ s.r.o.	Czech Republic
29	Fresenius Kabi s.r.o.	Czech Republic
30	Fresenius Kabi S.A.	Ecuador
31	Fresenius Kabi Scientific Office - Egypt	Egypt
32	Fenwal France S.A.S.	France
33	Fresenius Kabi France S.A.S.	France
34	Fresenius Kabi Groupe France S.A.S.	France
35	Fresenius Vial S.A.S.	France
36	Fresenius HemoCare GmbH	Germany
37	Fresenius Kabi AG	Germany
38	Fresenius Kabi Deutschland GmbH	Germany
39	Fresenius Kabi Logistik GmbH	Germany
40	medi1one Medical GmbH	Germany
41	MC Medizintechnik GmbH	Germany
42	Fresenius Kabi Ltd.	United Kingdom
43	Calea U.K. Ltd.	United Kingdom

44	Fresenius Kabi Hellas AEE	Greece
45	Fresenius Kabi Asia Pacific Ltd.	Hong Kong
46	Fresenius Kabi Hongkong Ltd.	Hong Kong
47	Fresenius Kabi Hungary Kft.	Hungary
48	Fresenius Kabi India Pvt. Ltd.	India
49	Fresenius Kabi Oncology Limited	India.
50	PT. Fresenius Kabi Indonesia	Indonesia
51	PT. Fresenius Kabi Combiphar	Indonesia
52	Fresenius Kabi Ltd, Ireland branch.	Ireland
53	Fresenius HemoCare Italia S.r.l.	Italy
54	Fresenius Kabi Italia S.r.l.	Italy
55	Fresenius Kabi iPSUM S.r.l.	Italy
56	Fresenius Kabi Japan K.K.	Japan
57	Fresenius Kabi Korea Ltd.	South Korea
58	Fresenius Kabi Baltics UAB	Lithuania
59	Fresenius Kabi Malaysia Sdn Bhd	Malaysia
60	Fresenius Kabi México, S.A. de C.V.	Mexico
61	Fresenius Kabi Nederland B.V.	Netherlands
62	Fresenius HemoCare Netherlands B.V.	Netherlands
63	EnzyPep B.V.	Netherlads
64	Fresenius Kabi NZ Ltd.	New Zealand
65	Fresenius Kabi Norge A/S	Norway
66	Fresenius Kabi Pakistan (Private) Limited	Pakistan
67	Fresenius Kabi Peru SA	Peru
68	Fresenius Kabi Philippines Inc.	Philippines
69	Fresenius Kabi Polska Sp. z o.o.	Poland
70	Fresenius Kabi Business Services Sp.z.o.o.	Poland
71	DOM Medica Sp. z o.o.	Polen
72	Clinico Medical Sp. z o.o.	Poland
73	Fresenius Kabi Pharma Portugal Lda.	Portugal
74	Labesfal - Laboratórios Almiro, S.A.	Portugal
75	Fresenius Kabi Romania S.R.L.	Romania
76	Fresenius Kabi LLC	Russian Federation
77	Fresenius Kabi d.o.o. Beograd	Serbia

78	Fresenius Kabi (Singapore) Pte Ltd.	Singapore

79	Fresenius Kabi South Africa (Pty) Ltd.	South Africa
80	Fresenius Kabi Manufacturing SA (Pty) Ltd.	South Africa
81	Fresenius Kabi Grupo España S.L.	Spain
82	Fresenius Kabi España S.A.U.	Spain
83	Quantium Medical S.L.U.	Spain
84	Fresenius Kabi AB , Sweden	Sweden
85	Fresenius Kabi AB, Finish branch	Finland
86	Fresenius Kabi AB, Denmark branch	Denmark
87	Fresenius Kabi (Schweiz) AG	Switzerland
88	Fresenius Kabi SwissBioSim GmbH	Switzerland
89	FresuCare AG	Switzerland
90	Fresenius Kabi Taiwan Ltd.	Taiwan
91	Fresenius Kabi (Thailand) Ltd.	Thailand
92	Fresenius Kabi Tunisia S.a.r.l.	Tunisia
93	Fresenius Kabi İlaç San. ve Tic. Ltd. Şti.	Turkey
94	Fresenius Kabi Middle East FZ-LLC	United Arab Emirates
95	Fresenius Kabi Latin America Exports S.A	Uruguay
96	Fresenius Kabi, LLC	United States
97	Fresenius Kabi USA, LLC	United States
98	Fenwal Inc.	United States
99	Fresenius Kabi Vietnam Joint Stock Company	Vietnam
100	Representative office of Fresenius Kabi Asia Pacific Limited	Vietnam
101	Fresenius SE & Co. KGaA	Germany
102	Fresenius Digital Technology GmbH	Germany
103	Fresenius Versicherungsvermittlungsgesellschaft mbH	Germany
104	Fresenius Management SE	Germany
105	Hyginus Publisher GmbH	Germany
106	Fresenius Digital Technology Polska sp. z o.o	Poland

107	Fresenius Netcare Beijing Consulting Co.,Ltd	China
108	Fresenius Digital Technology India Private Limited	India
109	Fresenius Immobilien-Verwaltungs-GmbH	Germany
110	FPS Immobilien Verwaltungs GmbH	Germany
111	Fresenius ProServe GmbH	Germany
112	Fresenius Finance Ireland PLC	Ireland
113	Fresenius Finance Ireland II PLC	Ireland
114	Fresenius Finance Holdings Ltd	Ireland
115	Fresenius Kabi Business Services Manila Inc	Philippines
116	GH Genhelix, S.A. (Unipersonal),	Spain
117	Mabxience Research, S.L. (Unipersonal),	Spain
118	Mabxience, S.A.U.	Argentina
119	Mabxience, S.A	Switzerland
120	Mabxience Holding, S.L.,	Spain

Schedule 2: Nature of Personal Data Transferred

The following Personal Data are subject to Transfers under the BCR for the following purposes:

Human Resources

The following Personal Data of managers, Employees and applicants of a Party may be Transferred to other Parties for the purposes described herein:

Purpose	Data categories
• Employment relationship administration • Employee IT and communication administration and operation • External communications and website • Workflow and performance management, sanctions • Knowledge and learning management • Salary management/payroll/benefits/pensions • Staff and resources planning • Recruitment, career development and staffing • Internal communications, intranet • Mergers and Acquisitions • Compliance, regulatory requirements •	• Identification data and personal characteristics (name, age, gender, nationality, national ID number, picture and contact details) • Terms of employment, qualifications, job description • Financial data (payroll, insurance, tax, pensions and benefits) • Work planning and performance (workflow, projects and assignments; hours worked; appraisal; sanctions) • Activity in trade unions or works council • Health conditions • Communication and IT use • Compliance investigations • Information on legal disputes • Police certificates (provided that those have no entries)

Customer

The following Personal Data of customers and contact persons of customers of a Party may be Transferred to other Parties for the purposes described below:

Purpose	Data categories
• Performance of agreements/manufacturing, provision and delivery of products and services/complaint handling • Customer relationship administration • Financials/invoicing/payment collection/ accounting • Marketing/customer relationship and account management • Mergers and acquisitions • Fulfilment of Compliance and regulatory requirements such as Business partner due diligence, sanction list screening, antimoney laundering, secure supply chain, customs and export law, tracing of products, credit risk rating	• Name, function, position and contact details • Business of customer • Business transactions and relationship with customer • Financial data (banking and invoicing) • Communication and IT use • Details related to public filings, trade registers and professional boards

Patients

The following Personal Data of patients and assistive persons (e.g. carers) of a Party may be Transferred to other Parties for the purposes described below:

Purpose	Data categories
• Performance of agreements/manufacturing, provision and delivery of products and services/complaint handling • Patients relationship administration • Marketing/patients relationship and account management • Financials/invoicing/payment collection/accounting • Compliance and regulatory requirements • Mergers and Acquisitions • Clinical Trials, Research and development • Emergency handling/adverse events and vigilance	• Identification data and personal characteristics (name, age, gender, nationality and contact details) • Medical records and health conditions • Treatment and relationship with patient • Financial data (banking and invoicing) • Communication and IT use

Supplier

The following Personal Data of supplier and contact persons of suppliers of a Party may be Transferred to other Parties for the purposes described below:

Purpose	Data categories
• Marketing/supplier relationship management • Supplier relationship administration • Performance of agreements/manufacturing, provisioning and delivery of products and services/complaint handling • Financials/invoicing/accounting • Mergers and Acquisitions • Fulfilment of compliance and regulatory requirements such as Business partner due diligence, sanction list screening, antimoney laundering, secure supply chain, customs and export law, tracing of products, credit risk rating	• Name, function, position and contact details • Business of supplier • Business transactions and relationship with supplier • Financial data (banking and invoicing) • Communication and IT use • Details related to public filings, trade registers and professional boards

Other Purposes

The following Personal Data of other Individuals (e.g. emergency contacts, press contacts) may be Transferred to other Parties for the purposes described below:

Purpose	Data categories

- Emergency handling,
- IT
- Security
- Regular mail administration, monitoring

- Name and contact details
- Connection to Fresenius or a Fresenius Individual
- Other information necessary for the purpose.