Binding Corporate Rules Policy

Novo Nordisk

Contents

Appendices to the BCR:

- Appendix 1 (Data Subjects' Rights Procedure)
- Appendix 2 (Audit Protocol)
- Appendix 3 (Complaint Handling Procedure)
- Appendix 4 (Co-operation Procedure)
- Appendix 5 (Updating Procedure)
- Appendix 6 (List of Participating Novo Nordisk Entities)
- Appendix 7 (Overview of Covered Processing Activities)
- Appendix 8 (Referenced Articles of the GDPR)

1 Introduction

This document contains the provisions of the Novo Nordisk Binding Corporate Rules ("BCR") for the protection of personal data which are binding for all participating corporate entities within the Novo Nordisk group towards data subjects, by virtue of third-party beneficiary rights.

Protecting the security and privacy of personal data is important to Novo Nordisk and Novo Nordisk conducts its business in compliance with applicable laws on data protection and data security.

The BCR are internal rules adopted by Novo Nordisk A/S, CVR-nr. 24256790, Novo Alle 1, 2880 Bagsvaerd, and its participating corporate entities set out in Appendix 6 (List of Participating Novo Nordisk Entities), having signed a legally binding Undertaking to present "adequate safeguards for the protection of the privacy and fundamental rights and freedoms of individuals" within the meaning of applicable data protection law, especially the data protection laws of the Member States of the European Economic Area ("EEA").

In the event of any conflict or inconsistency between the BCR Policy and the Appendices, the BCR Policy shall prevail.

2 Definitions

In the BCR Policy and the Appendices, the wording and expressions have the meanings ascribed to them in the GDPR. In addition to the terms used in the GDPR, terms written with a capital letter will have the meaning as ascribed to them below:

Term	Definition
Adequate Third Country	Means countries outside the EEA **with** an Adequacy Decision approved by the European Commission, based on Article 45 of the GDPR.
Audit Protocol	Means the audit protocol set out in Appendix 2 (Audit Protocol)
BCR	Means the Novo Nordisk Binding Corporate Rules – Controller (BCR-C), including its Appendices and the Undertaking, constituting an appropriate safeguard as defined in Article 47(2)(b) of the GDPR, providing a transfer mechanism for data transfers from controllers covered by the geographical scope of the GDPR to other controllers or processors within the same group, but established in Third Countries.
BCR Lead	Means The Danish Supervisory Authority (in Danish "Datatilsynet") acting as the lead supervisory authority in relation to approval and updates of the BCR under Article 47 of the GDPR, see Appendix 8 (Referenced Articles of the GDPR).

Binding Corporate Rules	Means Binding Corporate Rules as an appropriate safeguard as defined in Article 47(2)(b) of the GDPR.
Business Ethics Committee	The purpose of the Business Ethics Committee is to ensure oversight of business ethics and compliance, including with data privacy and the BCRs. The Business Ethics Committee reports to the Executive Management. Novo Nordisk Headquarters CEO and President is a member of the Business Ethics Committee.
Competent EEA Supervisory Authority	Means the independent public authority which is competent with regards to the exporting Novo Nordisk Entity. See the definition of 'EEA Supervisory Authority' below.
Complaint Handling Procedure	Means the complaint handling procedure set out in Appendix 3 (Complaint Handling Procedure).
Consent	Means any freely given specific, informed, and indication of the data subject's wishes by which the data subject signifies this agreement to personal data relating to them being processed. Conditions for a valid Consent are set forth in Article 7 of the GDPR, see Appendix 8 (Referenced Articles of the GDPR)
Co-operation Procedure	Means the co-operation procedure set out in Appendix 4 (Co-operation Procedure).
The Data Ethics & Privacy Advice team (DEPA)	Means the team in Novo Nordisk Headquarters responsible for developing and driving the global data protection and data ethics compliance programme in Novo Nordisk, advising and supporting Local Data Ethics Responsibles. DEPA is among other things also responsible for supporting the operational execution of the tasks of the DPO.
Data subjects' Rights Procedure	Means the procedure on the data subjects rights of access, rectification, restriction of processing, erasure of personal data and data portability as well as the right to object and not being subject to a decision based solely on automated processing set out in Appendix 1 (Data subjects' rights procedure).
DPO	Means the global Data Protection Officer appointed by Novo Nordisk Headquarters.
EEA	Means the European Economic Area.
EEA Supervisory Authority	Means an independent public authority which is established by a Member State pursuant to

	Article 51 of the GDPR, see Appendix 8 (Referenced Articles of the GDPR).
EU	Means the European Union.
GDPR	Means the 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 also known as the General Data Protection Regulation, applicable as of 25 May 2018.
Group Internal Audit (GIA)	Means Novo Nordisk internal audit function responsible for, among other things, audit of the adherence to BCR.
Local Data Ethics Responsible	Means the local employee(s) responsible for 1st line support and advice in a specific line of business, handling complaints etc. in a Novo Nordisk Entity.
Local or Regional Legal and Compliance	Means the local or the regional Legal and Compliance functions responsible for the local data protection program for a Novo Nordisk Entity or for the privacy program for a region of Novo Nordisk Entities.
Local Legislation	Means any applicable statutory legislation, regulations, statutes, court orders, practices, or mandatory standards in a non-EEA country.
Member State	Means a country within the EU and the EEA (following the GDPR's incorporation into the EEA Agreement on 6th July 2018).
Novo Nordisk	Means Novo Nordisk A/S and its subsidiaries owned and controlled directly or indirectly as a group, which are participating in the BCR from time to time, having duly signed the Undertaking and listed in Appendix 6 (List of participating Novo Nordisk Entities).
Novo Nordisk Entity	Means any Novo Nordisk Entity, individually, participating in the BCR listed in Appendix 6 (List of participating Novo Nordisk Entities). If more than one Novo Nordisk Entity is referred to, all having duly signed the Undertaking and listed in Appendix 6, they can also be referred to as Novo Nordisk Entities.
Novo Nordisk Headquarters	Means Novo Nordisk A/S, established in Denmark (within the EEA).
Other Third Country	Means countries outside of the EEA **without** an Adequacy Decision approved by the

	European Commission, based on Article 45 of the GDPR.
Undertaking	Means the legally binding instrument under which the Novo Nordisk Entities are obliged to adhere to the BCR.
Updating Procedure	Means the updating procedure set out in Appendix 5 (Updating procedure).
Special Categories of Personal Data	Means the categories of personal data listed in Article 9 GDPR, see Appendix 8 (Referenced Articles of the GDPR), as well as government identification numbers and criminal or civil offense, allegations or convictions.

3 About Novo Nordisk

Novo Nordisk is a leading global healthcare company, founded in 1923 and headquartered in Denmark. Our business is built around the Novo Nordisk Way, our commitment to be a sustainable business and our clear patient-centric purpose: driving change to defeat serious chronic diseases. For more information about Novo Nordisk please visit https://www.novonordisk.com/.

4 Scope of the BCR

The BCR apply to the Novo Nordisk Entities which are processing personal data relating to data subjects, including all Novo Nordisk Entities established:

a) in the EEA or in a country with an adequate level of data protection as acknowledged by a decision of the European Commission; and

b) outside the EEA or outside a country with an adequate level of data protection as acknowledged by a decision of the European Commission.

The BCR will cover personal data processed in connection with the following areas of Novo Nordisk' business: Research and Early Development, Development, Commercial Strategy & Corporate Affairs, People & Organisation, Rare Disease Operations, Product Supply, Quality & IT, Finance, Legal & Global Solutions and International Operations, as the data are transferred between the Novo Nordisk Entities. This includes data concerning minors (17 years old or younger), employees (current and/or former incl. their family members), healthcare professionals (incl. caregivers), job applicants, website visitors, suppliers, vendors, or other third parties incl. consultants, patients, clinical trial participants, and/or research subjects and government officials processed internally by the Novo Nordisk Entities as part of their regular business activities. Non-EEA Novo Nordisk entities covered will only adhere to the BCR and fulfil the obligations with respect to personal data transferred out of the EU or EEA under the BCR and not to any processing of personal data by the non-EEA Novo Nordisk Entity. All Novo Nordisk entities covered will adhere to the BCR and fulfil the obligations with respect to personal data transferred onwards if the data originated in the EU or EEA under the BCR.

The personal data will comprise of business contact information (e.g. name, email address, postal address, phone number), employment related information (e.g. job title, employment history, sick days, income, next of kin), financial information (e.g. taxes and debts), CVs, education or

qualifications, IP Address, IT user activity information and/or website usage data (e.g. cookies), age or date of birth and/or photo.

Novo Nordisk Entities may also process and transfer special categories of personal data between the Novo Nordisk Entities, namely Racial or ethnic origin, Political opinions, philosophical, or religious beliefs, Genetic or biometric data (for unique identification of a natural person, does not include photographs unless facial recognition technology is used), Physical or mental health data and/or Sex life or sexual orientation, government identification numbers, and criminal or civil offense allegations or convictions.

A detailed overview of the categories of data as well as the purposes relating to each category of data and its transfer is set out in Appendix 7 (Overview of covered processing activities).

5 Binding effect upon the Novo Nordisk Entities

The applicable Novo Nordisk Entities have undertaken to adhere to the BCR and have duly signed a legally binding Undertaking under which the Novo Nordisk Entities and their employees are obliged to adhere to the BCR. Accordingly, the applicable Novo Nordisk Entities and their employees are bound to comply with the BCR including all appendices hereto in respect of any transfer of personal data between Novo Nordisk Entities covered by the BCR.

The BCR will be referenced as a mandatory policy for employees to comply with internally in Novo Nordisk's OneCode - Principles for working at Novo Nordisk (Novo Nordisk Code of Conduct). Failure to comply with the BCR can lead to disciplinary sanctions.

Only the Novo Nordisk Entities covered by the scope and who have undertaken to adhere to BCR will fulfil the obligations set out herein.

6 Substantive principles for the processing of personal data

The following principles, which derive specifically from the GDPR, are part of Novo Nordisk Data Protection Policy and apply and will be enforced with respect to the processing of personal data within the scope of the BCR by any Novo Nordisk Entity:

6.1 Legitimacy and legality of data processing

The processing of personal data by a Novo Nordisk Entity is only permissible if at least one of the following prerequisites is fulfilled, which constitute an exhaustive list:

a) the data subject has given its unambiguous Consent;

b) data 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;

c) processing is necessary for the purposes of the legitimate interests pursued by the Novo Nordisk Entity or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data; or

d) processing is necessary for compliance with EU law or the law of the Member State to which the Novo Nordisk Entity is subject.

6.2 Purpose limitation

Personal data shall be collected for specified, explicit, and legitimate purposes and not be further processed in a way that is incompatible with those purposes. Novo Nordisk Entities are obligated to adhere to these original purposes when storing and further processing or using personal data transferred to them by another Novo Nordisk Entity.

The purpose of data processing may only be changed with the Consent of the data subject or to the extent permitted by applicable EU or Member State law. To the extent data is transferred from a Novo Nordisk Entity in an EEA country a Novo Nordisk Entity in a non-EEA country, the purpose of the processing may only be changed with the Consent of the data subject or to the extent permitted by the applicable law of the relevant Member State to which the Novo Nordisk Entity transferring the personal data is subject.

6.3 Transparency

Novo Nordisk commits to making the BCR readily available through the Novo Nordisk website and on the Novo Nordisk intranet.

All Novo Nordisk Entities shall process personal data in a transparent manner. All Novo Nordisk Entities will adhere to the substantive principles for processing personal data set out in Clause 6 and will ensure that data subjects are provided with the information set out under Clause 6.1 by the relevant Novo Nordisk Entity (in consultation with the transferring company, if applicable). Further, all Novo Nordisk Entities respect and act in accordance with the third-party beneficiary rights set out in Clause 8.

6.4 Accuracy, data minimisation and data retention

Personal data must be accurate and, where necessary, kept up to date. Appropriate measures are to be taken to ensure that inaccurate or incomplete personal data is corrected, restricted, or erased.

Data processing shall be guided by the principle of data minimisation according to which personal data collected shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. In particular, the Novo Nordisk Entities will make use of the possibility to anonymise or pseudonymise data, provided that the cost and effort involved corresponds with the desired purpose. Statistical evaluations or studies based on anonymised data are not relevant for data protection purposes.

Personal data, which is no longer required for the specified, explicit, and legitimate purposes, is to be erased or irreversibly anonymised in accordance with proportional operational principles and practices. In the event that statutory retention periods apply, the data shall be either pseudonymised or anonymised, if possible, rather than erased.

6.5 Onward transfer of data

The transfer of personal data from a Novo Nordisk Entity to a non-Novo Nordisk Entity (i.e. a company that is not bound by the BCR) outside the EEA is only permissible under the following conditions:

a) the country is deemed to provide an adequate level of protection of personal data under Article 45 of the GDPR; or

b) the receiving entity demonstrates that it has an adequate level of protection for personal data within the meaning of Article 46 GDPR, e.g. by concluding an EU standard contract (Standard Contractual Clauses 2021/914/EU) or by concluding other appropriate contractual agreements between the transferring and the receiving entity in accordance with Article 46(3)(a) of the GDPR, and adopting any supplementary measures necessary to ensure an essentially equivalent protection of personal data transferred to third countries as in the EU, or

c) the transfer is otherwise permissible as defined in Article 46 of the GDPR, or

d) the transfer is permissible under the exceptions defined in Article 49 of the GDPR, to the extent such transfer is not massive, disproportionate, or indiscriminate.

The wording of Articles 45, 46, and 49 of the GDPR is set out in Appendix 8 (Referenced Articles of the GDPR).

If the receiving entity is a processor, the Novo Nordisk Entity acting as controller must further ensure that the conditions for engaging a processor set out in Clause 6.11 are satisfied.

6.6 Special categories of personal data

The Novo Nordisk Entities may, if required for the purpose of the relevant processing activity, process and transfer Special Categories of Personal Data, such as e.g. trade union membership and information on health such as allergies or work-related incidents. For the purposes of the BCR, Special Categories of Personal Data shall be interpreted in accordance with the definition set out in Article 9 of the GDPR and additionally government identification numbers and criminal or civil offense allegations or convictions.

Further, Member State law may set out further categories of personal data which under the local Member State law is considered a special category of personal data. Each Novo Nordisk Entity will ensure to check for itself whether such local law variations exist and will ensure compliance with the requirements for processing special categories of personal data set out in such local Member State law.

Processing of Special Categories of Personal Data by a Novo Nordisk Entity is only permitted where there is a legal basis for the processing in Article 6 of the GDPR and where one of the derogations for processing Special Categories of Personal Data set out in Article 9(2) of the GDPR applies together with this legal basis. The wording of Articles 6 and 9 of the GDPR is set out in Appendix 8 (Referenced Articles of the GDPR).

Particular precautions will be taken by each Novo Nordisk Entity if Special Categories of Personal Data are processed. In particular, the relevant Novo Nordisk Entities will, in accordance with the principle of data minimisation, assess whether Special Categories of Personal Data are required to fulfil the intended purpose. If the purpose of the processing can be fulfilled by other means, which does not include the processing of Special Categories of personal data, those purposes shall be fulfilled in that manner.

Further, the Novo Nordisk entities will ensure to apply enhanced security measures where special categories of personal data are processed in order to ensure a level of security appropriate to the risk in accordance with Article 32 of the GDPR, see Appendix 8 (Referenced Articles of the GDPR).

The DPO, the Data Ethics and Privacy Advice team or Local Legal and Compliance in the Novo Nordisk Entity shall be consulted prior to the processing of Special Categories of Personal Data.

6.7 Direct Marketing

The Novo Nordisk Entities will inform the data subjects of their right to object free of charge to the processing of the data subject's personal data for marketing purposes. In such cases, the Novo Nordisk Entities will refrain from contacting the data subjects who have opted out of receiving marketing information.

6.8 Automated individual decisions

If personal data is processed for the purpose of making automated individual decisions, the legitimate interests of the data subject must be ensured through appropriate measures and the data subjects must be provided with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Decisions which produce legal effects concerning the data subject or similarly significantly affects the data subject may not be reached exclusively based on an automated individual procedure designed to evaluate a data subject's personal characteristics. An exception applies only if the decision:

a) is taken in the course of entering into, or performance of a contract, between the data subject and the controller;

b) is authorised by applicable EU or Member State law which also lays down measures to safeguard the data subject's legitimate interests; or

c) is based on the data subject's explicit Consent.

In the cases referred to in points (a) and (c), the Novo Nordisk Entity shall implement the right for the data subject to obtain human intervention with the Novo Nordisk Entity, to express their point of view, and to contest the decision.

Automated individual decisions must not be based on Special Categories of Personal Data, unless:

a) the data subject has given explicit Consent to the processing of those data for one or more specified purposes, except where EU or Member State law provides that the prohibition to process the special category of personal data may not be lifted by the data subject's Consent; or

b) processing is necessary for reasons of substantial public interest, on the basis of EU or Member State law.

Notwithstanding the above, suitable measures to safeguard the data subject's rights and freedoms and legitimate interests must always be in place for automated decision-making based on Special Categories of Personal Data.

6.9 Data security

Novo Nordisk has established and documented an IT Security organisation and has integrated data security into the processes of this organisation. The Novo Nordisk Entities will take appropriate technical and organisational measures to ensure data security, which protects personal data against accidental or unlawful erasure, unauthorised use, alteration, loss, and destruction as well as protecting against unauthorised disclosure or unauthorised access. Having regard to the state of the art, the cost of implementation, and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected (data protection by design and by default). Such measures shall further ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed (data protection by design and by default). Special Categories of Personal Data shall be subject to enhanced security and protection measures.

Specific measures are used to ensure adequate protection of personal data, including admission controls, system access controls, data access controls, transmission controls, input controls, job controls, availability controls, and segregation controls.

All computers and mobile devices are password/passcode protected and managed through a device management register. The Novo Nordisk internal network has a firewall system to protect internal company content from unauthorised external access. Transmission of personal data within Novo Nordisk's own network is typically encrypted, to the extent that the nature and intended purpose of the personal data requires this.

Novo Nordisk has implemented a data protection breach procedure setting out how all personal data breaches must be reported to and procedures for how the Data Ethics and Privacy Advice team and the Novo Nordisk DPO must handle personal data breaches, including reporting such to the Novo Nordisk Business Ethics Committee incl. Novo Nordisk Headquarters CEO and President.

Furthermore, the data protection breach procedure sets out how Novo Nordisk will ensure to notify relevant EEA Supervisory Authorities without undue delay and no later than 72 hours after having become aware of the personal data breach and equally how Novo Nordisk will ensure to notify data subjects of a personal data breach without undue delay where the personal data breach is likely to result in a high risk to the rights and freedoms of the data subjects. Finally, any personal data breaches will be documented (comprising the facts relating to the personal data breach, its effects, and the remedial action taken) and the documentation will be made available to the EEA Supervisory Authority on request.

6.10 Confidentiality

Only Novo Nordisk employees, who are authorised by Novo Nordisk and have been specifically instructed in compliance with data protection requirements may collect, process, or use personal data. Access authorisation of the individual employee will be restricted according to the nature and scope of the particular field of activity. The employee is prohibited from using personal data for private purposes, and from transferring or otherwise making personal data available to unauthorised persons. Unauthorised persons in this context include, for example, other employees, to the extent that they do not require access to/to process the personal data to complete their specialist tasks. The confidentiality obligation continues beyond the end of the employment of the employee in question.

6.11 Commissioned data processing

When a Novo Nordisk Entity acting as controller commissions another legal entity (either another Novo Nordisk Entity or a third party) acting as a processor to process personal data, the following requirements will be observed:

a) the processor is carefully assessed and selected by the controller on the basis of the processor's ability to ensure the implementation and maintenance of necessary technical and organisational security measures required for complying with the BCR in relation to the processing of personal data;

b) the controller will ensure and regularly verify that the processor remains fully compliant with the agreed technical and organisational security requirements;

c) the performance of commissioned data processing must be regulated in a written agreement in which the rights and obligations of the processor are unambiguously defined. In particular, such agreement will stipulate that the processor:

   i. processes the personal data only on documented instructions from the controller;

   ii. ensures the confidentiality of persons processing the personal data;

   iii. will not engage another processor without prior authorisation from the controller;

   iv. takes all measures required to implement the necessary technical and organisational security measures;

   v. ensures that any processing by a sub-processor will be subject to the same data protection requirements as stipulated in the agreement between the controller and the processor;

   vi. assists the controller with answering requests from data subjects to exercise their rights;

   vii. that the processor remains liable to the controller for any breach of the data protection obligations by a sub-processor;

   viii. assists the controller in ensuring compliance with applicable security requirements, notification of EEA Supervisory Authorities and data subjects in case of a data breach and with conducting data protection impact assessments and prior consultations with EEA Supervisory Authorities if necessary;

   ix. at the choice of the controller deletes or returns all copies of the personal data to the controller upon termination of the services;

   x. makes available to the controller all information necessary to demonstrate compliance with data protection legislation, in particular, the processor will contribute to audits, including inspections, conducted by the controller or a third party appointed by the controller; and

d) the controller retains responsibility for the legitimacy of the processing and continues to be the point of contact for the data subject.

6.12 Records of Processing Activities

Each Novo Nordisk Entity has established and maintains a record of all categories of processing activities carried out by the Novo Nordisk Entity. The record(s) of processing activities contain the following information for each processing activity:

a) the name and contact details of the Novo Nordisk Entity;

b) the purposes of the processing;

c) a description of the categories of data subjects and of the categories of personal data;

d) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in countries outside of the EEA;

e) where transfers of personal data to a recipient in countries outside of the EEA, the country(-ies) in which the recipient is established, and the documentation of suitable safeguards (e.g. the European Commission's Standard Contractual Clauses);

f) where possible, the envisaged time limits for erasure of the different categories of data; and

g) where possible, a general description of the technical and organisational security measures implemented to protect the personal data.

The record is maintained electronically, in writing, and will be made available to an EEA Supervisory Authority on request.

6.13 Data Protection Impact Assessments

Novo Nordisk assesses the risks of its processing activities (either through each Novo Nordisk Entity or through its use of overarching Novo Nordisk digital solutions).

Where it is assessed that a processing activity is likely to result in a high risk to the rights and freedoms of natural persons the responsible Novo Nordisk Entity will carry out a data protection impact assessment in accordance with Article 35 the GDPR, see Appendix 8 (Referenced Articles of the GDPR).

If the data protection impact assessment indicates that the processing would result in a high risk despite measures taken to mitigate the risk, the Local Legal and Compliance or Local Data Ethics Responsible must consult the Data Ethics and Privacy Advice team and the DPO. And the DPO who will consult the competent EEA Supervisory Authority, prior to processing personal data for the relevant processing activity.

6.14 Organisational control

Beyond the technical measures concerning the processing of personal data within the scope of the BCR, Novo Nordisk has implemented organisational measures to comply with the requirements of the GDPR which includes:

a) maintaining complete and up-to-date processing records of all processing activities;

b) having evidence of completed training of employees in data handling readily available;

c) having records and evidence of all employee agreements on confidentiality and data secrecy;

d) implementing the BCR with different supplementary policies across Novo Nordisk;

e) establishing and operating a comprehensive security framework (technical and organisational);

f) regularly updating the security framework;

g) having clear operating instructions / guidelines / leaflets in writing on correct data processing;

h) properly documenting all processing procedures;

i) conducting and logging prior assessments for higher-risk processing; and

j) establishing segmentation of functions within the IT sector at Novo Nordisk.

7 Essential rights of the data subject

7.1 Information obligations

7.1.1 Data obtained from the data subject.

Except where the data subject already has the information, each Novo Nordisk Entity will, at the time when personal data are obtained, provide data subjects (from whom personal data relating to the data subject is collected) with at least the following information:

a) the identity and contact details of the controller and its representative, if any;

b) the contact details of Novo Nordisk's DPO and the relevant Novo Nordisk Entity, as applicable;

c) the purpose(s) of the processing and the legal basis for the processing;

d) where the processing is based on a balancing of interests, the legitimate interest pursued by the relevant Novo Nordisk Entity;

e) the recipients or categories of recipients; and

f) where applicable, the fact that the Novo Nordisk Entity intends to transfer personal data to a Third Country and the existence or absence of an adequacy decision by the European Commission, or, where the transfer is based on appropriate safeguards, reference to those safeguards and the means by which to obtain a copy of or more information on such appropriate safeguards.

In addition, each Novo Nordisk Entity will provide the following information to the data subject, insofar as such information is relevant and necessary to ensure fair and transparent processing:

g) the period for which the personal data will be stored or if that is not possible, the criteria used to determine that period;

h) the existence of the right to request access to, rectification or restriction of and/or erasure of personal data as well as the right to object to the processing and the right to data portability;

i) where a processing is based on Consent, the right to withdraw such Consent;

j) the right to lodge a complaint with an EEA Supervisory Authority;

k) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, including whether the data subject is obliged to provide the personal data as well as the possible consequences of failure to provide such personal data; and

l) whether automated decision-making will be applied to the personal data, including information on the logic involved in such decision-making and the significance and envisaged consequences of such processing.

Where Novo Nordisk Entity intends to process personal data for a different purpose than that for which the personal data were originally collected, the Novo Nordisk Entity in question will notify the data subject prior to that further processing on the purpose of such processing and provide the data subject with any other relevant information pursuant to Clause 7.1.

7.1.2 Data not obtained from the data subject.

Where the data has not been obtained from the data subject and where the data subject does not already have the information, each Novo Nordisk Entity will provide the data subject with at least the following information:

a) the identity and contact details of the Novo Nordisk Entity and its representative, if any;

b) the contact details of Novo Nordisk's DPO and the relevant Novo Nordisk Entity, as applicable;

c) the purpose(s) of the processing and the legal basis for the processing;

d) the categories of personal data concerned;

e) the recipients or categories of recipients; and

f) where applicable, the fact that the controller intends to transfer personal data to a Third Country and the existence or absence of an adequacy decision by the European Commission, or, where the transfer is based on appropriate safeguards, reference to those safeguards and the means by which to obtain a copy of or more information on such appropriate safeguards.

In addition, each Novo Nordisk Entity will provide the following information to the data subject, insofar as such information is relevant and necessary to ensure fair and transparent processing:

g) the period for which the personal data will be stored or if that is not possible, the criteria used to determine that period;

h) where the processing is based on a balancing of interests, the legitimate interest pursued by the relevant Novo Nordisk Entity;

i) the existence of the right to request access to, rectification or restriction of and/or erasure of personal data as well as the right to object to the processing and the right to data portability;

j) where a processing is based on Consent, the right to withdraw such Consent;

k) the right to lodge a complaint with an EEA Supervisory Authority;

l) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; and

m) whether automated decision making will be applied to the personal data, including information on the logic involved in such decision making and the significance and envisaged consequences of such processing.

Each Novo Nordisk entity will provide the information set out in Clause 7.1.2:

a) within a reasonable period after obtaining the personal data, but no later than within one (1) month;

b) where the personal data are to be used for communication with the data subject, at the latest when the Novo Nordisk entity in question is first communicating to/with the data subject; and

c) if disclosure to a third party is envisaged, at the latest when the personal data is first disclosed to such third party.

Where a Novo Nordisk Entity intends to process personal data for a different purpose than that for which the personal data were originally collected, the Novo Nordisk Entity in question will notify the data subject prior to that further processing on the purpose of such processing and provide the data subject with any other relevant information pursuant to Clause 7.1.2.

7.2 Exceptions to the Information Obligation

7.2.1 The data subject will not have a right to information under the following circumstances:

a) when provided for by EU or Member State law to which the Novo Nordisk Entity is subject in accordance with Article 23 of the GDPR, see Appendix 8 (Referenced Articles of the GDPR);

b) the data subject already has the information;

c) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to complying with and implementing alternative measures as regulated by EU or Member State law;

d) if obtaining or disclosure of the personal data is expressly laid down by EU or Member State law to which the relevant Novo Nordisk Entity is subject, and which provides appropriate measures to protect the data subject's legitimate interests;

e) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by EU or Member State law; or

f) where the processing of personal data is necessary for conducting internal investigations for the purpose of e.g. fraud prevention or whistleblowing.

If the data subject believes that it has not been given all of the relevant information pursuant to Clause 7.1, the data subject can contact the respective Novo Nordisk Entity via the Local Legal and Compliance function, the Data Ethics and Privacy Advice team or the DPO of Novo Nordisk to request any further information as set out in Clause 7.1**.**

7.3 Rights of the data subjects

7.3.1 The rights.

Under the BCR, data subjects have the following rights in relation to the collection and processing of their personal data in accordance with Chapter III of the GDPR:

a) Right of access (see Clause 7.2.2(a));

b) Right to rectification (see Clause 7.2.2(b));

c) Right to erasure (see Clause 7.2.2(c);7.2.2(d));

d) Right to restriction of processing (see Clause 7.2.2(d));

e) Right to data portability (see Clause 7.2.2(e));

f) Right to object (see Clause 7.2.2(f)); and

g) Right not to be subject to automated individual decision-making, including profiling (see Clause 7.2.2(g)).

The rights of the data subject may in certain circumstances not apply, where EU or Member State law provides for a derogation from the right of the data subject, e.g. disproportionate or illegitimate requests or where there is a risk of disclosing confidential information or a risk of violation of the rights and freedoms of others. The subject matter of the above rights is explained in further detail in Clause 7.3.2.

7.3.2 Procedures for each right. To ensure the rights of the data subject, Novo Nordisk will ensure that all data subjects will be able to obtain:

a) **Right of access.** Confirmation as to whether or not personal data relating to the data subjects is being processed and at least the following information:

i. the purposes of the processing;

ii. the categories of personal data concerned;

iii. the recipients or categories of recipients to whom the personal data are disclosed, in particular recipients in third countries or international organisations;

iv. the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

v. the existence of the right to request from Novo Nordisk, rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

vi. the right to lodge a complaint with an EEA Supervisory Authority;

vii. where the personal data are not collected from the data subject, any available information as to their source;

viii. whether automated decision-making will be applied to the personal data, including information on the logic involved in such decision making and the significance and envisaged consequences of such processing; and

ix. where personal data are transferred to a Third Country or an international organisation, the appropriate safeguards relating to the transfer pursuant to Article 46 of the GDPR, see Appendix 8 (Referenced Articles of the GDPR).

Communication to the data subject shall be made in an intelligible form of the above information pertaining to the right of access. The right of access shall not adversely affect the rights and freedoms of others.

b) **Right to rectification.** Rectification of inaccurate personal data, without undue delay, concerning the data subject. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

c) **Right to erasure.** Erasure of personal data, without undue delay, where:

i. the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed;

ii. the data subject withdraws Consent and where there is no other legal ground for the processing;

iii. 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 of the data subject's personal data for direct marketing purposes;

iv. the personal data have been unlawfully processed;

v. the personal data have to be erased for compliance with a legal obligation in EU or Member State law to which the controller is subject; and

vi. the personal data have been collected in relation to the offer of information society services directly to a child.

Sub-clauses (i)-(vi) shall not apply to the extent that processing is necessary for exercising the right of freedom of expression and information, for compliance with a legal obligation which requires processing by EU or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or where processing is necessary for reasons of public interest in the area of public health in accordance with Article 9 of the GDPR, see Appendix 8 (Referenced Articles of the GDPR), or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in compliance with EU or Member State law or for the establishment, exercise or defence of legal claims.

d) **Right to restriction of processing.** Restriction of a Novo Nordisk Entity's processing of the data subject's personal data where one of the following apply:

i. the accuracy of the personal data is contested by the data subject, for a period enabling the Novo Nordisk Entity to verify the accuracy of the personal data;

ii. the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

iii. the Novo Nordisk Entity 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; and

iv. the data subject has objected to processing, pending the verification of whether the legitimate grounds of the Novo Nordisk Entity override those of the data subject (see Clause (f)).

e) **Right to data portability.** The right to data portability, means the right (i) to receive personal data concerning the data subject in a structured, commonly used and machine-readable format and (ii) to transmit those data to another controller without hindrance from the Novo Nordisk Entity to which the personal data have been provided, where:

i. the processing of personal data is based on a Consent or the processing of personal data is necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract; and

ii. the processing is carried out by automated means.

The data subject has the right to have the personal data transmitted directly from one controller to another, where technically feasible, and data portability shall be without prejudice to the right to erasure (see Clause c)).

The right to data portability shall furthermore not apply to processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Lastly, the right to data portability shall not adversely affect the rights and freedoms of others.

f) **Right to object.** The right at any time to (i) object, on grounds relating to the data subject's particular situation, where the processing of personal data is based on legitimate interests of the Novo Nordisk Entity or of a third party, including profiling based on legitimate interests and where the processing of personal data is for scientific or historical research purposes or statistical purposes pursuant to Article 89(1) of the GDPR and (ii) the right to object to the processing of the data subject's personal data for direct marketing purposes, including profiling to the extent that it is related to such direct marketing.

Where the data subject objects to processing;

i. based on legitimate interests, the Novo Nordisk Entity shall no longer process the personal data unless compelling legitimate grounds for the continued processing, which override the interests, rights and freedoms of the data subject can be demonstrated, or for the establishment, exercise, or defence of legal claims;

ii. for scientific or historical research purposes or statistical purposes pursuant to Article 89(1) of the GDPR, the Novo Nordisk Entity shall no longer process the personal data the processing is necessary for the performance of a task carried out for reasons of public interest; or

iii. for direct marketing purposes, the personal data shall no longer be processed for such purposes.

At the latest at the time of the first communication with the data subject, the right to object, including for direct marketing purposes, shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise their right to object by automated means using technical specifications.

g) **Right not to be subject to automated individual decision-making, including profiling.** The right not to be subject to a decision based solely on automated processing,

including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject.

The law of a Member State may restrict the data subject's rights set out above, including the right to access.

The Novo Nordisk Entities will ensure to provide the information set out in Clause 7.3.2 free of charge. However, where requests from a data subject are manifestly unfounded or excessive, in particular, because of their repetitive character, the Novo Nordisk Entity receiving a data subject access request may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested or refuse to act on the request.

The Novo Nordisk Entity acting as the controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

The Novo Nordisk Entities who have disclosed any personal data to third parties will notify such third parties of any rectification, erasure, or restriction carried out in accordance with Clause 7.2.2 (b), (c), or (d), unless this proves impossible or involves a disproportionate effort, without constraint, at reasonable intervals, and without excessive delay or expense. The response may be in a written form (email is sufficient).

The data subject can assert the abovementioned rights by contacting the respective Novo Nordisk Entity, the Data Ethics and Privacy Advise team, or the DPO.

8 Liability and Third-party beneficiary rights

The Novo Nordisk Headquarters (Novo Nordisk A/S) are the Liable BCR Member. Meaning that if a BCR member outside the EEA violates the BCR, the courts or other judicial authorities in the EEA will have jurisdiction, and data subjects will have the rights and remedies against the Novo Nordisk Headquarters as if the violation had been caused by the latter in the Member State in which it is based, instead of the BCR member outside the EEA.

Data subjects, whose personal data is (i) transferred from the EEA to a country outside the EEA by a Novo Nordisk Entity and (ii) is subject to the BCR, shall thus be able to enforce the following third-party beneficiary rights against such Novo Nordisk Entity as applicable:

a) the right to seek enforcement of compliance with the BCR, including its appendices, including but not limited to seeking enforcement of the following rights and principles:

   i. the substantive principles for the processing of personal data set out in Clause 6;

   ii. the rights of the data subject set out in Clause 7.3;

   iii. applicable Local Legislation in accordance with Clause 18;

   iv. the right to make a complaint through the procedure set out in Appendix 3 (Complaint Handling Procedure); and

v. any support of or co-operation needed with EEA Supervisory Authorities pursuant to Clause 15.

b) the right to lodge a complaint with an EEA Supervisory Authority of competent jurisdiction, in particular in the Member State of the data subject's:

i. habitual residence;

ii. place of work; or

iii. where the alleged infringement of the BCR occurred.

c) the right to an effective judicial remedy, where the data subject considers that their rights under the BCR have been infringed as a result of processing of their personal data in non-compliance with the BCR, by taking action, either independently or via representation by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of the GDPR, against Novo Nordisk in order to enforce compliance with the BCR in the courts of the jurisdiction in which:

i. the Novo Nordisk Entity responsible for the alleged breach is established;

ii. the data-exporting Novo Nordisk Entity is established; or

iii. the data subject has their habitual residence.

d) the right to make complaints to a Novo Nordisk Entity and where appropriate, receive compensation from a Novo Nordisk Entity for damage suffered as a result of a breach of the BCR in accordance with the determination of a court or other competent authority. Such complaints may be made in accordance with Appendix 3 (Complaint Handling Procedure);

e) the right to judicial remedies, the right to obtain redress and, where appropriate, compensation from any Novo Nordisk Entity in case of any breach of the BCR by that Novo Nordisk Entity. Further, in case of any damages resulting from a breach of the BCR by a Novo Nordisk Entity established outside the EEA, the data subject shall be able to enforce the third-party beneficiary rights under the BCR against the Novo Nordisk Headquarters as if the violation of the BCR had been caused by the Novo Nordisk Headquarters in the Member State where the Novo Nordisk Headquarters is established; and

f) the right to have easy access to the BCR. In this regard, each Novo Nordisk Entity commits to make the BCR readily available to every data subject and the BCR will be available on the Novo Nordisk global website.

The data subject may exercise its rights under Clause 8 by contacting Novo Nordisk as described in Clause 19 or by using the contact details set out in Appendix 3 (Complaint Handling Procedure).

9 Burden of proof

In the event of a claim being made in which a data subject, covered by the BCR, has suffered damage, where that data subject can establish facts to show that it is likely that the damage has occurred

because of a breach of the BCR, Novo Nordisk has agreed that the burden of proof to show that (i) a Novo Nordisk Entity outside the EEA is not responsible for the breach, or (ii) that no such breach took place, will rest with the Novo Nordisk Headquarters.

The Novo Nordisk Headquarters has undertaken to accept responsibility for and agreed to take the necessary action to remedy the acts of other Novo Nordisk Entities outside of the EEA when processing personal data covered by the BCR and to pay compensation for any material or non-material damages resulting from the violation of the BCR by Novo Nordisk Entities bound by the BCR.

10 Survival of third-party beneficiary rights

In the event that a non-EEA Novo Nordisk Entity is no longer a party to the BCR or otherwise ceases to exist, the non-EEA Novo Nordisk Entity will continue to apply the BCR requirements to the processing of personal data transferred to it by means of the BCRs, unless the non-EEA Novo Nordisk Entity, at the choice of the data-exporting Novo Nordisk Entity, deletes or returns the personal data to the data-exporting Novo Nordisk Entity. The non-EEA Novo Nordisk Entity will upon the data-exporting Novo Nordisk Entity request provide documentation for the deletion of personal data.

If Local Legislation applicable to the non-EEA Novo Nordisk Entity prohibits the return or deletion of personal data, the non-EEA Novo Nordisk Entity will continue to ensure compliance with the BCR and will only process the personal data to the extent and for as long as required under that Local Legislation.

11 Compliance and supervision of compliance

Novo Nordisk has appointed a DPO who is responsible for overseeing/monitoring and ensuring/advising on compliance with the BCR. The DPO advises the board of management, deals with the EEA Supervisory Authorities' investigations and annual reports on compliance, and ensures compliance at a global strategic level. The DPO shall not have any tasks that could result in a conflict of interests, such as but not limited to carrying out data protection impact assessment. The DPO is enjoying the support of management of Novo Nordisk for fulfilling these tasks reporting directly to the Business Ethics Committee incl. Novo Nordisk Headquarters CEO and President in regard to the BCR.

Novo Nordisk has further appointed a Data Ethics and Privacy Advice team to, among other things, support the operational execution of the tasks of the DPO, handling data breaches, data subject requests and complaints from data subjects.

Novo Nordisk has further appointed Local or Regional Legal and Compliance functions, which are designated for most of the Novo Nordisk Entities. The Local or Regional Legal and Compliance functions are responsible for reporting major privacy issues to the DPO, monitoring training, and implementing compliance at a local level. The Local or Regional Legal and Compliance further support the DPO and the Data Ethics and Privacy Advice team, which are responsible for overseeing and enabling compliance with the BCR on a day-to-day basis.

12 Procedure on the data subjects' rights

The Novo Nordisk Entities will comply with the Procedure on the data subjects' rights set out in Appendix 1 (Data Subjects' Rights Procedure).

13 Audit

The Novo Nordisk Entities will comply with the Audit Protocol set out in Appendix 2 (Audit Protocol).

14 Complaint process

The Novo Nordisk Entities will comply with the Complaint Handling Procedure set out in Appendix 3 (Complaint Handling Procedure).

If a complaint is considered justified either by the Novo Nordisk Entity or at the level of the DPO on appeal, they will as appropriate inform the data subject thereof and arrange for the necessary steps to be taken by the affected Novo Nordisk Entity in order to correct the matter at hand and in order to implement corrective actions for the future at the affected and other Novo Nordisk Entities.

15 Co-operation with the EEA Supervisory Authorities

The Novo Nordisk Entities will co-operate and support any EEA Supervisory Authorities in the event of inquiries, and/or complaints from data subjects concerning potential non-compliance with the BCR in accordance with the Co-operation Procedure set out in Appendix 4 (Co-operation Procedure).

16 Update of the BCR

The Novo Nordisk Entities will comply with the Updating Procedure set out in Appendix 5 (Updating procedure).

17 Training

The Novo Nordisk Entities will provide appropriate training to employees who have permanent or regular access to personal data, and who are involved in the collection of personal data or in the development of tools used to process personal data.

An extended learning program is rolled out for the key stakeholders and a general program for the remaining group of employees. The learning program entails a standard training for all employees and specific trainings for certain job functions. The standard training is for all job functions and must be completed in the onboarding process and bi-annually for all employees, and covers, among other things, producers of managing request for access to personal data by public authorises. For specific trainings the frequency varies depending on the course module and job function. Both the standard and the specific training materials shall be kept up to date. The Data Ethics and Privacy Advice (DEPA) team maintains and updates the standard training material. The specific training materials are maintained and updated by either DEPA or Local or Regional Legal and Compliance, depending on the targeted job functions. The training is generally supported by various awareness activities, such as articles and presentations on the Novo Nordisk intranet or through posters in buildings.

18 Relationship between BCR and Local Legislation

The BCR establishes a commitment that members will use it as a framework for data transfers only after thoroughly assessing the laws and practices in the third country of destination that are relevant to the processing of personal data by the data-importing BCR member.

Assessment of Local Legislation. Prior to a data transfer taking place, the data-exporting Novo Nordisk Entity with help of the data-importing Novo Nordisk Entity will assess if any Local

Legislation applicable to the Novo Nordisk Entities will prevent the data-importing Novo Nordisk Entity from fulfilling its obligations under the BCR.

When conducting such assessment, the data-exporting Novo Nordisk Entity will take into account the circumstances of the transfer and envisaged onward transfers, including the purpose of processing, the purpose of the transfer, the types of Novo Nordisk Entities involved, categories and format of personal data, location of the processing and storage, as well as the transmission channels used and the economic sector in which the transfer or set of transfers occur. Additionally, the entities will evaluate any obligations to disclose data to public authorities or provide access to data during transit, as well as the applicable limitations and safeguards and determine relevant supplementary contractual, technical, and/or organizational safeguards.

Updates to Local Legislation. The data-exporting Novo Nordisk Entity will in collaboration with the data-importing Novo Nordisk Entity monitor, on an ongoing basis, developments in applicable Local Legislation that could affect the level of protection.

Before any updated Local Legislation comes into force and where the transfer already takes place, the data-exporting Novo Nordisk Entity, with help from the data-importing Novo Nordisk Entity, will evaluate if the updated Local Legislation will prevent the Novo Nordisk Entities from fulfilling their obligations under the BCR and determine any required supplementary measures to be taken.

The DPO and the Data Ethics and Privacy Advice team will review and advise on the documented investigation and any proposed supplementary measures.

Higher level protection under Local Legislation. Where Local Legislation requires a higher level of protection than is contemplated under this BCR, such Local Legislation will take precedence over this BCR, and the processing will be carried out in accordance with the Local Legislation. Similarly, Local Legislation that respects the essence of the fundamental rights and freedoms and does not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR, see Appendix 8 (Referenced Articles of the GDPR), is not in contradiction with the BCR.

Local Legislation affecting obligations under the BCR. Where a data-importing Novo Nordisk Entity has reasons to believe that any Local Legislation the Novo Nordisk Entity is or may become subject to in a Third Country prevents or may prevent the Novo Nordisk Entity from fulfilling its obligations under the BCR or has or may have substantial effect on the guarantees provided by the applicable Local Legislation, the data-importing Novo Nordisk Entity will promptly inform the DPO, and, with guidance from the Data Ethics and Privacy Advice team, the data-exporting Novo Nordisk Entity.

Where possible, the data-importing Novo Nordisk Entity should notify the DPO, the data-exporting Novo Nordisk Entity and the data subject(s) if it receives a legally binding request from a public (including judicial) authority, under the law of the Third Country of destination for disclosure of personal data transferred pursuant to BCR.

Similarly, the data-importing Novo Nordisk Entity should notify the DPO, the data-exporting Novo Nordisk Entity and the data subject(s), if it becomes aware of any direct access by public authorities to such personal data, in accordance with the law of the Third Country of destination. If, despite its best efforts, the data importing Novo Nordisk Entity is not in a position to notify the DPO of specific

disclosure requests, it should provide the DPO with as much relevant information as possible on the requests. In addition, the data-importing Novo Nordisk Entity should provide the DPO with aggregate information at regular intervals.

The notification to the DPO and data-exporting Novo Nordisk entity must include information about the personal data requested, the requesting authority, the legal basis for the request, and the response provided. If necessary, the data-exporting Novo Nordisk Entity will help the data-importing Novo Nordisk Entity with the notification of the data subjects.

In specific cases where the abovementioned notification is prohibited, the relevant data-importing Novo Nordisk Entity will use its best efforts for such prohibition to be waived. If, despite its efforts, the requested Novo Nordisk Entity is not in a position to notify the data-exporting Novo Nordisk entity, it will on request provide general information on the requests it received to the data-exporting Novo Nordisk entity.

The data importing Novo Nordisk Entity is obliged to document the best efforts referred to above and to present this documentation to the data-exporting Novo Nordisk Entity, the liable Novo Nordisk Entity and the DPO without undue delay. Where there is a conflict between Local Legislation and the commitments in the BCR, the DPO will escalate this to the executive management of Novo Nordisk Headquarters who will make a responsible decision on what action to take and will consult the competent EEA Supervisory Authority(-ies) in case of doubt.

Assessment of supplementary measures. Where the evaluation of Local Legislation requires supplementary measures, the data-exporting Novo Nordisk Entity, together with the liable Novo Nordisk Entity and the DPO, will promptly identify appropriate measures to be adopted and implemented by the Novo Nordisk Entities. However, if no supplementary measures can be put in place, Novo Nordisk Entities must suspend the transfer. If (i) the transfers are not resumed within one month of suspension, (ii) the data-importing Novo Nordisk Entity is in substantial or persistent breach of the BCR, or (iii) the data-importing Novo Nordisk Entity fails to comply with a binding decision of a competent court or EEA Supervisory Authority regarding its obligations under the BCR, the data-importing Novo Nordisk Entity will, at the choice of the data-exporting Novo Nordisk Entity, return or destroy the personal data transferred prior to the suspension. The data-importing Novo Nordisk Entity will upon the data-exporting Novo Nordisk Entity request provide documentation for the deletion of personal data.

The outcome of the evaluation and proposed supplementary measures will be (i) informed to the other Novo Nordisk Entities (ii) properly documented and (iii) kept at the disposal of the EEA Supervisory Authority(-ies), on request.

Where the data-exporting Novo Nordisk Entity, along with the Liable BCR member(s) and DPO, assesses that the BCR – even if accompanied by supplementary measures – cannot be complied with for a transfer or set of transfers, or if instructed by the Competent Supervisory Authority, it commits to suspend the transfer or set of transfers at stake, 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.

The data-exporting Novo Nordisk Entity shall end the transfer or set of transfers if the BCR cannot be complied with and compliance with the BCR is not restored within one month of suspension. In this case, personal data that has been transferred prior to the suspension, and any copies thereof, should,

at the choice of the data-exporting Novo Nordisk Entity, be returned to it or destroyed in their entirety.

Request for disclosure in a Third Country. Where a data-importing Novo Nordisk Entity receives a request for disclosure from a public authority, the data-importing Novo Nordisk Entity will review the legality of such request, in particular, whether it remains within the powers granted to the requesting public authority. If the data-importing Novo Nordisk Entity, after careful assessment, concludes that there are reasonable grounds to consider that the request is unlawful under the Local Legislation of the country of destination, applicable obligations under international law, and principles of international comity, the data-importing Novo Nordisk Entity will challenge the request and pursue possibilities of appeal. When challenging a request, the data-importing Novo Nordisk Entity will seek interim measures to suspend the effects of the request until the competent judicial authority has decided on its merits. Also, the data-importing Novo Nordisk Entity will not disclose the personal data requested until required to do so under the applicable procedural rules and will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

In any event, the Novo Nordisk Entities will ensure that any transfers of personal data to any public authority are not massive, disproportionate, and indiscriminate in a manner that it would go beyond what is necessary in a democratic society.

The outcome of the review, assessment, and challenge mentioned above will be (i) informed to the other Novo Nordisk Entities (ii) properly documented, and (iii) kept at the disposal of the competent EEA Supervisory Authority(-ies), on request.

19 Non-Compliance and Enforcement

This Non-Compliance Clause outlines the critical commitments associated with the BCRs as established by Novo Nordisk. These requirements are applicable to the entirety of the BCR framework and encompass all data processing activities that fall within its scope and applies to all Novo Nordisk Entities forming part of the BCRs.

Binding Commitment. The data-exporting Novo Nordisk Entity shall not transfer personal data under the BCR framework to any BCR member unless such BCR member is effectively bound by the BCR and demonstrates the capability to deliver compliance with the provisions herein. Each BCR member is required to acknowledge and enforce these commitments across their operations.

Notification of Inability to Comply. The data-importing Novo Nordisk Entity must promptly inform the data-exporting Novo Nordisk Entity of any circumstances preventing compliance with the BCR, regardless of the reason. This includes, but is not limited to, events such as changes in local legislation, operational challenges, or other unforeseen factors. Notice must be provided without undue delay and should include details of the nature, extent, and anticipated duration of the non-compliance.

Suspension of Data Transfer. In the event that the data-importing Novo Nordisk Entity is found to be in breach of the BCR or is unable to comply with the obligations stipulated within it, the data-exporting Novo Nordisk Entity shall suspend any further transfers of personal data. Such suspension

shall take effect immediately upon notification to the data-importing Novo Nordisk Entity and shall remain in effect until compliance is restored.

Return or Deletion of Data. The data-importing Novo Nordisk Entity shall, at the discretion of the data-exporting Novo Nordisk Entity, immediately return or delete all personal data transferred under the BCR without delay, if the data transfer in suspended, or in circumstances where:

- compliance with the BCR is not restored within a reasonable timeframe, and in any event within one month of suspension;
- the data-importing Novo Nordisk Entity is in substantial or persistent breach of the BCR; or
- the data-importing Novo Nordisk Entity fails to comply with a binding decision from a competent court or Competent Supervisory Authority regarding obligations under the BCR.

This obligation extends to any and all copies of the data maintained in any form, whether electronic, paper, or other formats.

Certification of Deletion. Following the return or deletion of personal data, the data-importing Novo Nordisk Entity must provide written certification to the data-exporting Novo Nordisk Entity confirming that all personal data has been fully removed from all systems, databases, and records, thereby ensuring no residual data remains.

Continued Compliance. Until such time as all transferred personal data has been deleted or returned, the data-importing Novo Nordisk Entity remains wholly obligated to ensure continued compliance with the BCR. This entails ongoing implementation of necessary safeguards and monitoring protocols to prevent any further breaches of compliance.

Local Law Compliance. In instances where local laws applicable to the data-importing Novo Nordisk Entity prohibit the return or deletion of the transferred personal data, the data-importing Novo Nordisk Entity warrants that it will continue to ensure adherence to the BCR for the duration of the data processing. The data-importing Novo Nordisk Entity commits to carrying out only those processing activities that are strictly necessary as per the applicable local law and shall refrain from further processing of the personal data beyond these requirements.

Impact of Local Laws. For circumstances where local laws and/or practices affect compliance with the BCR, please refer to Section 18 above. This section outlines specific conditions, obligations, and alternative measures to be taken to maintain compliance with the BCR framework despite potential conflicts with local legislation.

20 Contact

The Novo Nordisk has policies and procedures in place to oversee and ensure compliance with all aspects of this BCR. The governance on a local level of the BCR is the responsibility of the Local Legal and Compliance reporting to the Data Ethics and Privacy Advice team and the DPO.

Data subjects can raise any concerns with a Local Legal and Compliance function of the relevant Novo Nordisk Entity, if one such is designated, or with the DPO:

Novo Nordisk A/S
Novo Alle 1
DK-2880 Bagsvaerd
Denmark
Email: Privacy@novonordisk.com
Website: https://www.novonordisk.com/data-privacy-and-user-rights.html

Appendix 1

Data Subject's Rights Procedure
to the Novo Nordisk Binding Corporate Rules

1 Introduction

1.1 The GDPR gives data subjects whose personal data is being processed in scope of the geographical and material scope of the GDPR, the right to be informed of whether any personal data about them is being processed and access to such data ("Data Subject Rights").

1.2 Data subjects whose personal data is processed or transferred between Novo Nordisk Entities, as defined in the BCR, will also benefit from the Data Subject Rights. This procedure explains how Novo Nordisk deals with a Data Subjects Rights Request relating to such personal data (referred to as "Request" in this procedure).

1.3 A data subject making a Request to a Novo Nordisk Entity under this procedure is entitled to:

a) Be informed whether the Novo Nordisk Entity is processing personal data about that data subject.

b) Be given at least the following information:

i. the purposes of the processing,

ii. the categories of personal data concerned,

iii. the recipients or categories of recipients to whom the personal data are disclosed, in particular recipients in Third Countries or international organisations,

iv. the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period,

v. the existence of the right to Request from the Novo Nordisk Entity, acting as a controller, rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing,

vi. the right to lodge a complaint with an EEA Supervisory Authority,

vii. the right at any time to object to the processing of personal data concerning the data subject, on grounds relating to the data subject's particular situation, where the processing of personal data is based on a balancing of interests, including against being subject to automated decision making such as profiling, which produces legal effects or significantly affects the data subjects,

viii. where personal data are transferred to a Third Country or to an international organisation, the appropriate safeguards pursuant to Article 46 of the GDPR, see Appendix 8 (Referenced Articles of the GDPR) relating to the transfer,

ix. where the personal data are not collected from the data subject, any available information as to their source, and

x. whether automated decision making will be applied to the personal data, including information on the logic involved in such decision making and the significance and envisaged consequences of such processing.

c) Communication in intelligible form of the personal data held by the Novo Nordisk Entity.

d) The rectification, erasure or restriction of personal data the processing of which does not comply with the provisions of the BCR or applicable law, in particular because of the incomplete or inaccurate nature of the data;

e) Erasure of personal data where:

i. the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed;

ii. the data subject withdraws consent and where there is no other legal ground for the processing;

iii.

iv. the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to processing of the data subject's personal data for direct marketing purposes;

v. the personal data have been unlawfully processed;

vi. the personal data have to be erased for compliance with a legal obligation in EU or Member State law to which the controller is subject;

vii. the personal data have been collected in relation to the offer of information society services directly to a child;

f) Notification to third parties to whom the data has been disclosed of any rectification, erasure or restriction carried out in compliance with Clause 7.2.2(b), (c), and (d) of the BCR Policy, unless this proves impossible or involves a disproportionate effort, without constraint, at reasonable intervals and without excessive delay or expense. The response may be in a written form (e-mail is sufficient);

g) Restriction of a Novo Nordisk Entity's processing of the data subject's personal data where:

i. the accuracy of the personal data is contested by the data subject, for a period enabling the Novo Nordisk Entity to verify the accuracy of the personal data;

ii. the processing is unlawful, and the data subject opposes the erasure of the personal data and Requests the restriction of their use instead;

iii. the Novo Nordisk Entity 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; or

the data subject has objected to processing pending the verification whether the legitimate grounds of the Novo Nordisk Entity override those of the data subject;

h) The right at any time to object, on grounds relating to the data subject's particular situation, where the processing of personal data is based on legitimate interests of the controller or of a third party, including profiling based on legitimate interests and processing by the controller. Further:

i. where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing;

ii. where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes;

iii. at the latest at the time of the first communication with the data subject, the right to object, including for direct marketing purposes, shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information;

iv. in the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

i) 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.

1.4 The data subject making a Request may do so in writing. Without excluding other means of communication, Requests may be in writing and can for an example be submitted via Novo Nordisk's web portal or by e-mail to Privacy@novonordisk.com. The Request must be made by the data subject to the DPO. The Data Ethics and Privacy Advice team assists the DPO with handling any such Request. Relevant contact information can be found in respective privacy notices and are also listed on Novo Nordisk website, https://www.novonordisk.com/data-privacy-and-user-rights.html.

1.5 The data subject making the Request is obliged to provide necessary information required to confirm its identity before the Request is processed by the relevant Novo Nordisk Entity, including specification of the Data Subject Rights the data subject wish to exercise. As a general rule, no fee will be applied by the Novo Nordisk Entities for the processing of the Request. Where Requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Novo Nordisk Entity receiving a data subject Request may charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested.

1.6 Subject to Article 1.5, a Novo Nordisk Entity must respond to a Request within one (1) month of receipt of the Request. The period may be extended by two further months where necessary, taking into account the complexity and number of Requests. The Data Ethics and Privacy Advice team must inform the data subject of any such extension within a maximum of four weeks of receipt of the Request, together with the reasons for the delay.

1.7 The Novo Nordisk Entity may ask for information which the Novo Nordisk Entity may reasonably require in order to confirm the identity of the data subject making the Request and to locate the information which that data subject seeks.

2 Procedure

2.1 Receipt of a Request

2.1.1 If any employee or subcontractor of a Novo Nordisk Entity receives any Request from a data subject regarding the processing of the data subject's personal data, they must pass on the Request to the Data Ethics and Privacy Advice team or the DPO immediately upon receipt, indicating the date on which the Request was received together with any other information, which may assist the Data Ethics and Privacy Advice team or DPO in dealing with the Request.

2.1.2 The Request does not have to be official or mention data protection law to qualify as a Data Subject Rights Request.

2.2 Initial Steps

2.2.1 The Data Ethics and Privacy Advice team will make an initial assessment of the Request to decide whether it is a valid Request according to applicable law and this procedure and whether, any further information, including confirmation of identity, is required.

2.2.2 The Data Ethics and Privacy Advice team will contact the data subject in writing to confirm receipt of the Request, seek confirmation of identity or further information, if required, or decline the Request if one of the exemptions to subject access applies.

2.3 Exemptions to Data Subject Rights:

2.3.1 A Request may be refused on the following grounds:

a) where the Request is made to a Novo Nordisk Entity established within the EEA, and

b) the Request relates to the use or collection of personal data by that Novo Nordisk Entity on a data subject covered by the GDPR, and

c) where the refusal to provide the information is consistent with the law of the Member State in which the Novo Nordisk Entity is established; or

d) where Request(s) from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character.

2.4 **The Search and the Response**

2.4.1 The Data Ethics and Privacy Advice team will, where necessary in cooperation with the relevant employees in the Novo Nordisk entity, arrange a search of relevant electronic and paper filing systems.

2.4.2 The personal data requested will be collated by the Data Ethics and Privacy Advice team into a readily understandable format (internal codes or identification numbers used at the Novo Nordisk Entity that correspond to personal data shall be translated before being disclosed). A cover letter will be prepared by the Data Ethics and Privacy Advice team which includes information required to be provided in response to a Request.

2.4.3 Where the provision of the information in permanent form is not possible or in cases where the interests of the data subject outweigh, the communication may, however, be given in the form of oral information about the contents of the data. In such circumstances the data subject may be offered the opportunity to have access to the information by inspection in attendance of a Novo Nordisk employee appointed by the Data Ethics and Privacy Advice team, or to receive the information in another form.

2.5 **Request for deletion, rectification or restriction of personal data**

2.5.1 If a Request is received for the deletion, rectification or restriction of that data subject's personal data, such a Request must be considered and dealt with as appropriate by the Data Ethics and Privacy Advice team.

2.5.2 If a Request is received advising of a change in that data subject's personal data, such information must be rectified or updated accordingly if the Novo Nordisk Entity is satisfied that there is a legitimate basis for doing so.

2.5.3 If the Request is to cease processing the data subject's personal data because the rights and freedoms of the data subject are prejudiced by virtue of such processing by a Novo Nordisk Entity, or on the basis of other compelling legitimate grounds, the matter will be assessed by the Data Ethics and Privacy Advice team and consult the DPO if necessary. Where the processing undertaken by a Novo Nordisk Entity is required by Member State law, the Request will not be regarded as valid. However, the Request from the data subject will in any case be dealt with and a reply will be provided to the data subject.

2.5.4 All queries and Requests relating to this procedure are to be addressed to the Data Ethics and Privacy Advice team or to the DPO.

3 Complaint handling

3.1.1 The data subjects whose personal data is collected or otherwise processed is entitled to file a complaint to an EEA Supervisory Authority of competent jurisdiction or with a court as described in Appendix 3 (Complaint Handling Procedure), even if they have not beforehand filed a complaint with the relevant Novo Nordisk Entity.

4 Further information and review procedure

4.1.1 If any more information about this procedure or any other aspect of Data Subject Rights is needed, please contact:

Novo Nordisk A/S
Novo Alle 1
DK-2880 Bagsværd
Denmark
E-Mail: Privacy@novonordisk.com
Website: https://www.novonordisk.com/data-privacy-and-user-rights.html

4.1.2 This procedure will be reviewed and considered in line with applicable laws and case law on Data Subject Rights cases and subject to procedures under the BCR.

Appendix 2
Audit Protocol
to the Novo Nordisk Binding Corporate Rules

1 Background

Novo Nordisk has adopted the BCR. The purpose of the BCR is to safeguard personal data transferred between- and processed by Novo Nordisk Entities. The BCR requires approval from the EEA Supervisory Authorities in the Member States from which the personal data is transferred. One of the requirements of the EEA Supervisory Authorities is that Novo Nordisk conduct audits according to audit procedures compliant with the BCR and relevant best practices and quality standards. This document describes how Novo Nordisk complies with this requirement.

2 Scope of audit

Group Internal Audit (GIA) performs a multitude of audits, including GDPR audits. The scope of the audits is designed to ensure that Novo Nordisk has implemented processes and controls ensuring that Novo Nordisk process the least amount of personal data needed to fulfil the purposes for which they have been collected, inform people about how their personal data is being processed, that personal data is only shared with those who needs access, that personal data is stored and transferred in a secure manner, and that personal data is deleted when no longer needed.

Such audit activities will inherently address compliance with all aspects of the BCR, including methods of ensuring that corrective and preventive actions will take place.

3 Responsibility for compliance

On a quarterly basis the Head of Group Internal Audit is responsible for bringing the result of the performed audits to the attention of the Audit Committee. The Audit Committee consists of representatives from the Board of Directors of Novo Nordisk Headquarters and their meetings are attended by the Chief Financial Officer (CFO), the Senior Vice President of Global Legal & Patents, and the Head of Group Internal Audit. They are all committed to ensuring that any corrective actions remedying any non-compliance will take place as soon as is reasonably possible. If an audit indicates material compliance issues, the CFO and the Chairman of the Audit Committee are responsible for communicating the result of the audit to the entire Board of Directors of Novo Nordisk Headquarters.

The global data protection organisation in Novo Nordisk is described in the Clause 11 of the BCR Policy.

4 Timing

Group Internal Audit (GIA) carries out rolling annual audits and additionally if requested by the DPO, Group Internal Audit (GIA) determines the Novo Nordisk Entities covered by and the scope of the audits based on a risk and on a materiality assessment. To ensure audit readiness, audits are both performed as announced and unannounced audits.

5 Auditors

GDPR audits are performed by Novo Nordisk's internal specialists in Group Internal Audit (GIA). Such audit teams both includes GDPR compliance experts as well as IT experts. Group Internal Audit (GIA) or the DPO may in some cases choose to use external auditors for example if the matter or process subject to audit (i) involves the function that would normally carry out the audit, or (ii) requires specific technical, legal - or other expert competencies. The DPO cannot conduct the audit if

it results in a conflict of interest. In such cases, the auditor should be determined by the Audit Committee.

6 Report

Group Internal Audit (GIA) will for each GDPR audit issue an audit report including mitigating actions. Group Internal audit (GIA) will follow up with the relevant Novo Nordisk Entity(-ies) to ensure that mitigating actions in such audit reports, i.e. corrective and preventive measures, are taken within the agreed deadlines.

Group Internal Audit (GIA) will provide copies of audit reports including mitigating actions to be taken based on the audit as required under the BCR to:

- The DPO;
- The board of the liable Novo Nordisk Entity(-ies) together with the DPO;
- On a quarterly basis to the Novo Nordisk Audit Committee; and
- Upon request and liaising with the DPO and the Data Ethics and Privacy Advice team, the competent EEA Supervisory Authorities.

Appendix 3

Complaint Handling Procedure
to the Novo Nordisk Binding Corporate Rules

1 Background

Novo Nordisk must implement a complaint handling procedure as part of the BCR. The purpose of this procedure is to explain how a complaint brought by a data subject whose personal data is processed by a Novo Nordisk Entity, is handled.

2 How to make a complaint

Data subjects can report complaints by contacting the DPO, please refer to Clause 20 of the BCR Policy for contact details. Further information on how to file complaints is available on the Novo Nordisk website https://www.novonordisk.com/data-privacy-and-user-rights.html.

Complaints are always forwarded to the relevant Local Data Ethics Responsible or Local Legal and Compliance. Without excluding other means of communication, complaints may be in writing and can for an example be submitted via Novo Nordisk's web portal or email Privacy@novonordisk.com.

3 Complaint handling by Novo Nordisk

The designated Local Data Ethics Responsible or Local Legal and Compliance will handle the complaint in a diligent and efficient manner and take all relevant steps to handle the complaint according to the BCR and the law of the Member State in which the Novo Nordisk Entity to which the complaint was submitted is established. The Local Data Ethics Responsible or Local Legal and Compliance is assisted by the Data Ethics and Privacy Advice team. The complaint handling procedure will include involving relevant employees within the Novo Nordisk Entities and, if necessary, by involving external advice.

4 Response time

The designated Local Data Ethics Responsible or Local Legal and Compliance will acknowledge receipt of a complaint to the data subject concerned, investigate and provide a substantive response without undue delay and in any case within one (1) month. The acknowledgement may be made by telephone followed up by a written confirmation. If, due to the complexity and number of requests a satisfactory response cannot be provided within this period, the Local Data Ethics Responsible or Local Legal and Compliance will inform the individual having filed a complaint, accordingly, including as to when a response can be expected. However, a response must be provided within (3) three months of receipt of the complaint. The local legal department may assist the Local Data Ethics Responsible or Local Legal and Compliance in communicating with the data subject.

5 When a complaint is found to be justified

If a complaint is considered justified, either by the Novo Nordisk Entity or by the DPO on appeal (see Clause 6), they will, as appropriate, inform the data subject. They will arrange for the necessary steps to be taken by the affected Novo Nordisk Entity to correct the matter and implement necessary corrective actions to the affected and other Novo Nordisk Entities.

The Novo Nordisk Entity will take appropriate remedial action without undue delay. This may include correcting or deleting personal data, updating records, modifying processing operations, or implementing additional safeguards. The complainant will be informed of the outcome in writing, including details of the corrective measures taken. Additionally, if necessary, the Novo Nordisk Entity or the DPO will inform Novo Nordisk Headquarters. Based on the findings, Novo Nordisk Headquarters will

assess whether systemic changes are required to prevent the complaint from reoccurring and document all steps taken to demonstrate compliance with the BBCRs and applicable data protection law. When applicable in accordance with Clause 8 of the BCRs as well as article 82 of the GDPR, Novo Nordisk will recognize the data subject's right to seek and obtain compensation for any material or non-material damage suffered as a result of the breach.

6 When a finding is not acceptable to the complainant

If the finding by a Novo Nordisk Entity is not acceptable and the complainant disputes the response of the Novo Nordisk entity or any aspect of a finding and notifies the Novo Nordisk Entity accordingly, the matter will be referred to the Data Ethics and Privacy Advice team and the Novo Nordisk DPO. The DPO and the Data Ethics and Privacy Advice team will review the matter and advise the complainant to either accept the original finding or will substitute a new finding. The DPO will respond to the complainant within one (1) month of the referral. As part of the review, the DPO may arrange to meet the parties in an attempt to resolve the complaint. The costs for this will be borne by the applicable Novo Nordisk Entity.

If the complaint is upheld, the DPO will arrange for any necessary steps to be taken as a consequence depending on the character of the complaint and the steps taken by the data subject.

Data subjects, whose personal data is transferred from the EEA in accordance with the BCR, have rights under the BCR to:

a) complain to an EEA Supervisory Authority; and/or

b) lodge an application with a court of competent jurisdiction,

if they are not satisfied with the way in which the complaint has been resolved. Individuals entitled to such rights will be notified accordingly as part of the complaints handling procedure and be given relevant information as how to lodge a complaint.

The data subjects whose personal data is collected or otherwise processed is entitled to file a complaint to an EEA Supervisory Authority of competent jurisdiction or with a court as stated above, even if they have not beforehand filed a complaint with the relevant Novo Nordisk Entity.

Appendix 4

Co-operation Procedure
to the Novo Nordisk Binding Corporate Rules

1 This Co-operation Procedure sets out the way in which the Novo Nordisk Entities will co-operate with the EEA Supervisory Authorities in relation to the BCR.

2 Where required, the Novo Nordisk Entities will make the necessary personnel available for dialogue with an EEA Supervisory Authority in relation to the BCR.

3 The Novo Nordisk Entities will:

a) Cooperate with competent EEA Supervisory Authorities and upon request, provide them with any information about the processing operations covered by the BCR-C;

b) Accept to be audited and to be inspected, including where necessary, on-site, by competent EEA Supervisory Authorities for the purpose of reviewing compliance with the BCR, in accordance with the applicable law of the Member State in which the Novo Nordisk Entity is located, or, in the case of a Novo Nordisk Entity located outside the EEA, in accordance with the applicable law of the Member State from which the personal data is transferred under the BCR;

c) Take into account the advice of competent EEA Supervisory Authorities; and

d) Abide by any legally binding decisions made by competent EEA Supervisory Authorities on any issue related to the BCR.

4 The DPO and the Data Ethics and Privacy Advice team will be responsible for liaising with the EEA Supervisory Authorities for the above purposes.

5 The Novo Nordisk Entities will provide upon request copies of the results of any audit of the BCR to an EEA Supervisory Authority of competent jurisdiction.

6 Each Novo Nordisk Entity commits to having any dispute related to the competent EEA Supervisory Authority's exercise of supervision of compliance with the BCR resolved by the courts of the Member State of the competent EEA Supervisory Authority in accordance with that Member State's procedural law and to the jurisdiction of that Member State's courts.

Appendix 5

Updating Procedure
to the Novo Nordisk Binding Corporate Rules

1 This Appendix 5 (Updating procedure) sets out how Novo Nordisk Headquarters will communicate changes to the BCR to the BCR Lead, data subjects and Novo Nordisk Entities.

2 Data Ethics and Privacy Advice team will:

a) Keep track of and record any updates to the BCR;

b) Maintain an up-to-date list of the Novo Nordisk Entities by updating Appendix 6 (List of participating Novo Nordisk Entities);

c) Ensure that all new Novo Nordisk entities, to be bound by the BCR, ascend by signing the Undertaking, and comply with the BCR before a transfer of personal data to them takes place; and

d) Provide necessary information to data subjects benefitting from the BCR and, upon request, to EEA Supervisory Authority.

3 Novo Nordisk Headquarters must, without undue delay and prior to implementation, communicate to the BCR Lead any changes or modifications, which may significantly affect the BCR or be detrimental to the level of protection offered by the BCR. Novo Nordisk Headquarters will also provide a brief explanation of the reasons for any such notified changes to the BCR.

4 Once a year, Novo Nordisk Headquarters will notify any changes made to the BCR and/or Appendix 6 (List of participating Novo Nordisk Entities) to the BCR Lead, with a brief explanation of the reasons for the changes, or confirmation that no changes have been made.

5 Novo Nordisk Headquarters will report any changes, without undue delay, to the BCR to Novo Nordisk Entities.

Appendix 7

Overview of Covered Data Processing Activities
to the Novo Nordisk Binding Corporate Rules

Processing activities	Purpose of processing	Categories of personal data	Categories of data subjects	Categories of recipients	Place of processing	Time limits for erasure	Legal basis for processing The wording of the respective articles is set out in Appendix 8 (Referenced Articles of the GDPR)
Research and Early Development (RE&D) & Development	• Adverse events and complaint handling; • Clinical operations and Clinical Research; • Data metrics insights and analytics; • Digital health; • Donations, grants & sponsorships; • Employee admin (including performance, benefits and compensation); • External communications; • Finance; • HCP education; • HCP engagement (including ToV,	**Ordinary categories:** • Business Contact Information (e.g. name, email address, postal address, phone number); • Employment related information (e.g. Job title, employment history, sick days, income); • Financial information (e.g. taxes and debts); • CVs, • Education or qualifications; • IP Address;	• Minors (17 years old or younger); • Employees (current and/or former ind. their family members); • HCPs (Healthcare Professionals, incl. caregivers); • Job Applicants; • Website visitors; • Suppliers, vendors, or other third parties incl. consultants; • Patients, clinical trial participants, and/or research subjects; • Government officials.	Novo Nordisk Entities as defined in the BCR and as listed in Appendix 6.	Data is collected at local sites and submitted directly to Novo Nordisk A/S's corporate systems. Data may be shared with central functions in HQ in Denmark or regional HQ in Switzerland, and with business support functions in India, Mexico, China, and USA. Data from clinical trials and other research activities are stored at the Novo Nordisk Entity being the sponsor of the trial/research activity.	Corporate retention systems in place where retention periods are defined for each processing activity based on legal and GxP requirements and subject to clause 6.4 of the BCR.	**Ordinary categories:** Article 6(1)(a)-(d) and (f) of the GDPR **Special categories:** Article 9(2)(a)-(c), (e)-(f), and (i)-(j) of the GDPR Local legal bases in the Member State or Third Country where a clinical trial/ research activity is conducted.

Processing activities	Purpose of processing	Categories of personal data	Categories of data subjects	Categories of recipients	Place of processing	Time limits for erasure	Legal basis for processing The wording of the respective articles is set out in Appendix 8 (Referenced Articles of the GDPR)
	speaker engagements, KOLs); • HCP Interactions (segmentation, CRM, MCM); • Health & Safety (incl. employees and public); • IT (security, access controls and systems); • Legal & compliance operations; • Market research; • Medical insights and publications; • Monitoring and auditing; • Patient education; • Patient engagement; • Patients Support/Assistance programs (PSPs, PAPs);	• IT user activity information and/or website usage data (e.g. cookies); • Age or date of birth; • Photo; **Special categories:** • Government Identification numbers • Racial or ethnic origin; • Political opinions, philosophical, or religious beliefs; • Genetic data • Biometric data (for unique identification of a natural person, does not include photographs unless facial recognition			Biosamples are mainly stored in Denmark. For the centralized pharmacovigilance system, data is mainly stored within the EU, India, China, and USA. Data may also to a limited extent be processed in the countries where the Novo Nordisk Entities are established (subject to applicable law) according to Appendix 6.		

Processing activities	Purpose of processing	Categories of personal data	Categories of data subjects	Categories of recipients	Place of processing	Time limits for erasure	Legal basis for processing The wording of the respective articles is set out in Appendix 8 (Referenced Articles of the GDPR)
	• Pre-clinical trial research; • Procurement and Supplier management; • Real world evidence and outcomes research; • Recruitment incl. Background checks; • Regulatory submissions and reporting; • Social media monitoring and use.	technology is used); • Physical or mental health data; • Sex life or sexual orientation.					
Commercial Strategy & Corporate Affairs (CSCA)	• Digital health; • External communications; • HCP education; • HCP engagement (including ToV, speaker engagements, KOLs);	**Ordinary categories:** • Business Contact Information (e.g. name, email address, postal address, phone number); • Employment related information (e.g.	• Minors (17 years old or younger); • Employees (current and/or former incl. their family members); • HCPs (Healthcare Professionals, incl. caregivers);	Novo Nordisk Entities as defined in the BCR and as listed in Appendix 6.	Data may be shared with central functions in HQ in Denmark or regional HQ in Switzerland, and with business support functions in India, Mexico, China, and USA.	Corporate retention systems in place where retention periods are defined for each processing activity based on local law requirements for keeping CRM data or business-related data, including local bookkeeping laws and	**Ordinary categories:** Article 6(1)(a)-(d) and (f) of the GDPR **Special categories:** Article 9(2)(a)-(c), and (e)-(f), of the GDPR

Processing activities	Purpose of processing	Categories of personal data	Categories of data subjects	Categories of recipients	Place of processing	Time limits for erasure	Legal basis for processing The wording of the respective articles is set out in Appendix 8 (Referenced Articles of the GDPR)
	• HCP Interactions (segmentation, CRM, MCM); • IT (security, access controls and systems); • Market research; • Medical insights and publications; • Patient education; • Patient engagement; • Patients Support/Assistance programs (PSPs, PAPs); • Real world evidence and outcomes research; • Social media monitoring and use; • Sales.	Job title, employment history, sick days, income); • IP Address; • IT user activity information and/or website usage data (e.g. cookies); • Age or date of birth; • Photo; **Special categories:** • Racial or ethnic origin; • Genetic or biometric data (for unique identification of a natural person, does not include photographs unless facial recognition technology is used);	• Website visitors; • Suppliers, vendors, or other third parties incl. consultants; • Patients, clinical trial participants, and/or research subjects; • Government officials.		For the centralized CRM system, data is mainly stored within Denmark, Switzerland, India, China, and USA. Data may also to a limited extent be processed in the countries where the Novo Nordisk Entities are established (subject to applicable law) according to Appendix 6.	subject to clause 6.4 of the BCR.	Local legal bases in the Member State or Third Country where a commercial activity is conducted.

Processing activities	Purpose of processing	Categories of personal data	Categories of data subjects	Categories of recipients	Place of processing	Time limits for erasure	Legal basis for processing The wording of the respective articles is set out in Appendix 8 (Referenced Articles of the GDPR)
		• Physical or mental health data.					
People & Organisation (P&O)	• Employee admin (including performance, benefits and compensation); • Recruitment incl. Background checks; • Health & Safety (incl. employees and public) • Monitoring and auditing; • Data metrics insights and analytics.	**Ordinary categories:** • Business Contact Information (e.g. name, email address, postal address, phone number); • Employment related information (e.g. Job title, employment history, sick days, income); • Financial information (e.g. taxes and debts); • IT user activity information and/or website usage data (e.g. cookies); • CVs, Education or qualifications;	• Minors (17 years old or younger); • Employees (current and/or former incl. their family members); • Suppliers, vendors, or other third parties incl. consultants; • Job Applicants; • Website visitors.	Novo Nordisk Entities as defined in the BCR and as listed in Appendix 6.	Data may be shared with central functions in HQ in Denmark or regional HQ in Switzerland, and with business support functions in India, Poland, Brazil, China, and USA. For the centralized HR systems, data is mainly stored within Denmark, Switzerland, India, China, and USA. Data may also to a limited extent be processed in the countries where the Novo Nordisk Entities are established (subject to applicable law) according to Appendix 6.	Corporate retention systems in place where retention periods are defined for each processing activity based on local law requirements, legal obligation or requirements in local collective agreements for keeping HR data, legal obligations, legitimate interests, business requirements etc. and subject to Clause 6.4 of the BCR	**Ordinary categories:** Article 6(1)(a)-(c) and (f) of the GDPR **Special categories:** Article 9(2)(a)-(b), and (e)-(f) of the GDPR Article 10 of the GDPR Local legal bases in the Member State or Third Country where the HR activity is conducted.

Processing activities	Purpose of processing	Categories of personal data	Categories of data subjects	Categories of recipients	Place of processing	Time limits for erasure	Legal basis for processing The wording of the respective articles is set out in Appendix 8 (Referenced Articles of the GDPR)
		• Age or date of birth; • Photo; • Other. **Special categories:** • Government Identification numbers; • Racial or ethnic origin; • Political opinions, philosophical, or religious beliefs; • Trade union membership; • Genetic or biometric data (for unique identification of a natural person, does not include photographs unless facial recognition technology is used);					

Processing activities	Purpose of processing	Categories of personal data	Categories of data subjects	Categories of recipients	Place of processing	Time limits for erasure	Legal basis for processing The wording of the respective articles is set out in Appendix 8 (Referenced Articles of the GDPR)
		• Physical or mental health data; • Sex life or sexual orientation; • Criminal or civil offense, allegations or convictions.					
Rare Disease Operations (RareD)	• Adverse events and complaint handling; • Data metrics insights and analytics; • Digital health; • Donations, grants & sponsorships; • Employee admin (including performance, benefits and compensation); • External communications; • Finance; • HCP education;	**Ordinary categories:** • Business Contact Information (e.g. name, email address, postal address, phone number); • Employment related information (e.g. Job title, employment history, sick days, income); • Financial information (e.g. taxes and debts); • CVs, Education or qualifications;	• Minors (17 years old or younger); • Employees (current and/or former incl. their family members); • HCPs (Healthcare Professionals, incl. caregivers); • Job Applicants; • Website visitors; • Suppliers, vendors, or other third parties incl. consultants; • Patients, clinical trial participants, and/or research subjects;	Novo Nordisk Entities as defined in the BCR and as listed in Appendix 6.	Data is collected at local sites and submitted directly to Novo Nordisk A/S's corporate systems. Data may be shared with central functions in HQ in Denmark or regional HQ in Switzerland, and with business support functions in India, Mexico, China, and USA. Data from clinical trials and other research activities are stored at the Novo	Corporate retention systems in place where retention periods are defined for each processing activity based on legal and GxP requirements and subject to clause 6.4 of the BCR.	**Ordinary categories:** Article 6(1)(a)-(d) and (f) of the GDPR **Special categories:** Article 9(2)(a)-(c), (e)-(f), and (h)-(j) of the GDPR Local legal bases in the Member State or Third Country where a clinical trial/ research activity is conducted.

Processing activities	Purpose of processing	Categories of personal data	Categories of data subjects	Categories of recipients	Place of processing	Time limits for erasure	Legal basis for processing The wording of the respective articles is set out in Appendix 8 (Referenced Articles of the GDPR)
	• HCP engagement (including ToV, speaker engagements, KOLs); • HCP Interactions (segmentation, CRM, MCM); • IT (security, access controls and systems); • Legal & compliance operations; • Market research; • Medical insights and publications; • Patient education; • Patient engagement; • Patients Support/Assistance programs (PSPs, PAPs); • Procurement and Supplier management;	• IP Address; • IT user activity information and/or website usage data (e.g. cookies); • Age or date of birth; • Photo. **Special categories:** • Government Identification numbers; • Racial or ethnic origin; • Genetic or biometric data (for unique identification of a natural person, does not include photographs unless facial recognition technology is used);	• Government officials.		Nordisk Entity being the sponsor of the trial/research activity. Data may also to a limited extent be processed in the countries where the Novo Nordisk Entities are established (subject to applicable law) according to Appendix 6.		

Processing activities	Purpose of processing	Categories of personal data	Categories of data subjects	Categories of recipients	Place of processing	Time limits for erasure	Legal basis for processing The wording of the respective articles is set out in Appendix 8 (Referenced Articles of the GDPR)
	• Real world evidence and outcomes research; • Recruitment incl. Background checks; • Social media monitoring and use.	• Physical or mental health data.					
Product Supply, Quality & IT (PSQIT)	• Production and manufacturing, incl. maintains and facility management; • IT (security, access controls and systems); • Monitoring and auditing; • Data metrics insights and analytics; • Procurement and Supplier management.	**Ordinary categories:** • Business Contact Information (e.g. name, email address, postal address, phone number); • Financial information (e.g. taxes and debts); • Employment related information (e.g. Job title, employment history, sick days, income);	• Government officials; • Patients, clinical trial participants, and/or research subjects; • Suppliers, vendors, or other third parties incl. consultants; • Website visitors; • Minors (17 years old or younger); • Employees (current and/or	Novo Nordisk Entities as defined in the BCR and as listed in Appendix 6.	Data may be shared with central functions in HQ in Denmark or regional HQ in Switzerland, and with business support functions in India, Mexico, China, and USA. For the centralized IT systems, data is mainly stored within Denmark, Switzerland, India, China, and USA. Data may also to a limited extent be	Corporate retention systems in place where retention periods are defined for each processing activity based on local law requirements and subject to Clause 6.4 of the BCR	**Ordinary categories:** Article 6(1)(a)-(d) and (f) of the GDPR **Special categories:** Article 9(2)(a)-(c), and (e)-(f), of the GDPR Article 10 of the GDPR

Processing activities	Purpose of processing	Categories of personal data	Categories of data subjects	Categories of recipients	Place of processing	Time limits for erasure	Legal basis for processing The wording of the respective articles is set out in Appendix 8 (Referenced Articles of the GDPR)
		• CVs, Education or qualifications; • Location tracking information and personal whereabouts; • IP Address; • IT user activity information and/or website usage data (e.g. cookies); • Age or date of birth; • Photo. **Special categories:** • Government Identification numbers; • Racial or ethnic origin; • Political opinions, philosophical, or religious beliefs; • Trade union membership;	former incl. their family members); • HCPs (Healthcare Professionals, incl. caregivers).		processed in the countries where the Novo Nordisk Entities are established (subject to applicable law) according to Appendix 6.		

Processing activities	Purpose of processing	Categories of personal data	Categories of data subjects	Categories of recipients	Place of processing	Time limits for erasure	Legal basis for processing The wording of the respective articles is set out in Appendix 8 (Referenced Articles of the GDPR)
		• Genetic or biometric data (for unique identification of a natural person, does not include photographs unless facial recognition technology is used); • Physical or mental health data; • Sex life or sexual orientation; • Criminal or civil offense, allegations or convictions.					
Finance, Legal & Global Solutions (FLGS)	• Finance incl. accounting and payroll handling; • Legal & compliance operations; • IT (security, access controls and systems);	**Ordinaty categories:** • Business Contact Information (e.g. name, email address, postal address, phone number);	• Employees (current and/or former incl. their family members); • Suppliers, vendors, or other third	Novo Nordisk Entities as defined in the BCR and as listed in Appendix 6.	Data may be shared with central functions in HQ in Denmark or regional HQ in Switzerland, and with business support functions in India, Mexico, China, and USA.	Corporate retention systems in place where retention periods are defined for each processing activity based on local law requirements and subject to Clause 6.4 of the BCR	**Ordinary categories:** Article 6(1)(a)-(d) and (f) of the GDPR **Special categories:** Article 9(2)(a)-(c), and (e)-(f), of the GDPR

Processing activities	Purpose of processing	Categories of personal data	Categories of data subjects	Categories of recipients	Place of processing	Time limits for erasure	Legal basis for processing The wording of the respective articles is set out in Appendix 8 (Referenced Articles of the GDPR)
	• Procurement and Supplier management; • Employee admin (including performance, benefits and compensation; • HCP engagement (including ToV, speaker engagements, KOLs).	• Employment related information (e.g. Job title, employment history, sick days, income); • CVs, Education or qualifications; • IP Address; • IT user activity information and/or website usage data (e.g. cookies).	parties incl. consultants; • HCPs (Healthcare Professionals, incl. caregivers).		For the centralized systems, data is mainly stored within Denmark, Switzerland, India, China, and USA. Data may also to a limited extent be processed in the countries where the Novo Nordisk Entities are established (subject to applicable law) according to Appendix 6.		
International Operations (IO)	• Employee admin (including performance, benefits and compensation); • Finance incl. accounting and payroll handling; • Health & Safety (incl. employees and public);	**Ordinary categories:** • Business Contact Information (e.g. name, email address, postal address, phone number); • Employment related information (e.g. Job title,	• Minors (17 years old or younger); • Employees (current and/or former incl. their family members); • HCPs (Healthcare Professionals,	Novo Nordisk Entities as defined in the BCR and as listed in Appendix 6.	Data may be shared with central functions in regional HQ in Switzerland or HQ in Denmark, and with business support functions in India, Mexico, China, and USA. For the centralized systems, data is	Corporate retention systems in place where retention periods are defined for each processing activity based on local law requirements and subject to Clause 6.4 of the BCR	**Ordinary categories:** Article 6(1)(a)-(d) and (f) of the GDPR **Special categories:** Article 9(2)(a)-(c), and (e)-(f), of the GDPR

Processing activities	Purpose of processing	Categories of personal data	Categories of data subjects	Categories of recipients	Place of processing	Time limits for erasure	Legal basis for processing The wording of the respective articles is set out in Appendix 8 (Referenced Articles of the GDPR)
	• Recruitment incl. Background checks; • Adverse events and complaint handling; • Clinical operations; • HCP engagement (including ToV, speaker engagements, KOLs); • HCP Interactions (segmentation, CRM, MCM); • Legal & compliance operations; • Market research; • Medical insights and publications; • Patient engagement; • Real world evidence and outcomes research.	employment history, sick days, income); • Financial information (e.g. taxes and debts); • CVs, Education or qualifications; • Age or date of birth; • Photo; • IP Address; • IT user activity information and/or website usage data (e.g. cookies); • Age or date of birth; • Photo. **Special categories:** • Government Identification numbers; • Physical or mental health data.	incl. caregivers); • Job Applicants; • Website visitors; • Patients, clinical trial participants, and/or research subjects.		mainly stored within Switzerland, Denmark, India, China, and USA. Data may also to a limited extent be processed in the countries where the Novo Nordisk Entities are established (subject to applicable law) according to Appendix 6.		

Appendix 8

Referenced Articles of the GDPR
to the Novo Nordisk Binding Corporate Rules

1 Appendix listing the GDPR articles specifically mentioned in Novo Nordisk's BCR.

In the event of a contradiction between the wording of the articles listed in Article of this Appendix 8 and the wording of the corresponding articles found in the official text of the GDPR, in the version existing at the time this BCR is approved, the official text of the GDPR shall prevail.

2 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 (General Data Protection Regulation):

2.1 Article 6 – Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) 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;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

2.2 Article 7 – Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

2.3 Article 9 – Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of 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 shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, 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 data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; L 119/38 EN Official Journal of the European Union 4.5.2016

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, 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 data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

2.4 Article 10 – Processing of personal data relating to criminal convictions and offences

1. Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

2.5 Article 23 – Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

2.6 Article 32 – Security of processing

1. 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, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

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

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

2.7 Article 35 – Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

2.8 Article 45 – Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided 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. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

2.9 Article 46 – Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

2.10 Article 47 – Binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

2.11 Article 49 – Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, 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:

(a) 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;

(b) 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;

(c) 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;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) 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;

(g) the transfer is made from a register which according to Union 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 Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

2.12 Article 51 – Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

2.13 Article 80 – Representation of data subjects

1. The data subject shall have the right to mandate 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, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

2.14 Article 89 – Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for

the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.