Novo Nordisk Binding Corporate Rules

for the protection of personal data transfers

Contents:

1 BACKGROUND AND OVERVIEW

1.1 Introduction to the Binding Corporate Rules

Novo Nordisk is committed to respectful processing of Personal Data in our business operations that complies with applicable Data Protection Laws. These Binding Corporate Rules ("BCRs") establish Novo Nordisk's approach to compliance with European Data Protection Laws and specifically to transfers of Personal Data that originates in Europe between the Novo Nordisk Entities. A list of the Novo Nordisk Entities covered by these BCRs are listed in Appendix 6. These BCRs also apply where Novo Nordisk Entities process Personal Data on behalf of other Novo Nordisk Entities.

1.2 Definitions

In the BCR, the expressions have the meanings ascribed to them in article 4 of the GDPR. In addition to the terms used in the GDPR, terms written with a capital letter will have the meaning ascribed to them below, which are also in line with the GDPR.

Term	**Definition**
Binding Corporate Rules or BCR	means the Novo Nordisk Binding Corporate Rules set out in this document, including its appendices and the Unilateral Declaration.
Consent	means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.
Data Subject's Requests and Complaint Handling Procedure	means the data subject's requests and complaint handling procedure set out in Appendix 1 of the BCR.
Europe	for the purpose of these BCRs reference to Europe refers to the European Economic Area ('EEA').
European Data Protection Laws or simply Data Protection Laws	means the General Data Protection Regulation and any national data protection legislation enacted by member states of the European Economic Area in accordance with the right granted to Member States under the GDPR.

General Data Protection Regulation	means the EU Regulation (EU) 2016/679 (General Data Protection Regulation) to be applied as of 25 May 2018.
List of Entities	means the list of Novo Nordisk Entities participating in the BCR as set out in Appendix 6 to the BCR.
Local Data Protection Responsible	means the Novo Nordisk employee or external counsel appointed to drive local data protection compliance for one or more Novo Nordisk Entities.
Member State	means a member state of the EEA.
Novo Nordisk	means Novo Nordisk A/S and its subsidiaries owned and controlled directly or indirectly, which are participating in the BCR from time to time.
Novo Nordisk Entity	means a Novo Nordisk entity participating in the BCR.
Novo Nordisk Headquarters	means Novo Nordisk A/S.
Personal Data	means any information relating to an identified or identifiable natural person as defined in article 4(1) of the GDPR.
Service Level Agreement (SLA)	means an agreement between a Novo Nordisk Entity acting as a service provider and another Novo Nordisk Entity acting as a service recipient that defines the level of service expected from the Novo Nordisk Entity acting as a service provider.
Special Categories of Personal Data	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic 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.
Supervisory Authority	means an independent public authority which is established by a Member State to oversee compliance with data protection legislation as defined in article 4(21) of the GDPR.
Updating Procedure	means the updating procedure set out in Appendix 4 of the BCR.

Unilateral Declaration	means the unilateral declaration signed by authorized signatories of Novo Nordisk A/S in order to make the BCR legally binding.

The following acronyms are used in the BCR:

BCR	Binding Corporate Rules
DPO	Data Protection Officer
DPR	Data Protection Responsible
EEA	European Economic Area
GDPR	General Data Protection Regulation

1.3 Scope of the BCR

Novo Nordisk BCR covers all transfers of Personal Data between Novo Nordisk Entities, where the Personal Data originates in Europe. This includes the initial transfer from a Novo Nordisk Entity in Europe to a Novo Nordisk Entity located outside Europe in a jurisdiction, which does not provide an adequate level of protection of Personal Data as acknowledged by a decision of the European Commission (a "third country"). Further, it includes the subsequent processing of the Personal Data by such Novo Nordisk Entity located in a third country.

The Personal Data transferred under the BCR will mainly concern the following types of data subjects: Novo Nordisk employees, healthcare providers, patients, contractors, and business contacts.

Further details about the scope of processing activities covered by the Novo Nordisk BCR, including the categories of Personal Data and types of processing activities for each type of data subjects are set out in Appendix 5 (Overview of data processing activities covered by the BCR).

1.4 Binding effect upon the Novo Nordisk Entities

The BCR apply to Novo Nordisk A/S and subsidiaries owned and controlled indirectly or directly by Novo Nordisk A/S and included in the list of participating entities set out in Appendix 6 to the BCR. All Novo Nordisk Entities participating in the BCR, 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.

Only the Novo Nordisk Entities included in the List of Entities set out in Appendix 6 to the BCR will fulfil the obligations set out herein. Non-EU 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.

1.5 Third party beneficiary rights

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 be able to enforce the following third-party beneficiary rights against such Novo Nordisk Entity:

- **Enforce compliance.** Seek enforcement of compliance with these BCRs, including its appendices, including but not limited to seeking enforcement of the following rights and principles:
    - The substantive principles for the processing of Personal Data set out in clause 2;
    - The rights of the data subject set out in clause 3;
    - Local statutory regulations insofar as such local law stipulates a higher level of protection of Personal Data than the BCR;
    - The right to make a complaint through the procedure set out in the Data Subjects' Requests Procedure;
    - Any support of or cooperation needed with European Supervisory Authorities.

- **Complain to Novo Nordisk.** Complain to a Novo Nordisk Entity established in Europe responsible for exporting the Personal Data in accordance with the Data Subject's Requests and Complaint Handling Procedure in Appendix 1 and seek appropriate redress from the Novo Nordisk Entity in Europe responsible for exporting the Personal Data including the remedy of any breach of the BCR by the non-European Novo Nordisk Entity.

- **Seek compensation.** To obtain redress and where appropriate, receive compensation from the Novo Nordisk Entity responsible for exporting the Personal Data or the Novo Nordisk Headquarter for any damage suffered as a result of a breach of the BCR by the non-European Novo Nordisk Entity importing the Personal Data.

- **Complain to a European Supervisory Authority.** Lodge a complaint with a European Supervisory Authority of competent jurisdiction, in particular in the Member State of the data subject's;
    - habitual residence;
    - place of work; or
    - where the alleged infringement of the BCR occurred.

- **Take judicial action.** Take action against a Novo Nordisk Entity in order to enforce compliance with the BCR in the courts of the jurisdiction in which the European Novo Nordisk Entity responsible for exporting the Personal Data to a Novo Nordisk Entity established in a non-European country is established or in the courts of the jurisdiction in which the data subject has his or her habitual residence either against the European Novo Nordisk Entity responsible for exporting the Personal Data or against the Novo Nordisk Entity established in a non-European country importing the Personal Data in order to enforce compliance with the BCR, including the appendices.

- **Copy of the BCR.** Obtain a copy of the BCR with its appendices and the Unilateral Declaration on request or by obtaining a copy of the BCR on Novo Nordisk's website.

Novo Nordisk agrees that the burden of proof to show that a Novo Nordisk Entity outside Europe is not responsible for the breach, or that no such breach took place, will rest with the European Novo Nordisk Entity responsible for exporting the Personal Data to a Novo Nordisk Entity outside Europe. For claims directed towards the Novo Nordisk Headquarter, the burden of proof will be on the Novo Nordisk Headquarter, regardless of which Novo Nordisk entity was responsible for the alleged breach.

In addition, claims may be brought against the Novo Nordisk Headquarter, which has undertaken to accept responsibility for and agreed to take the necessary action to remedy the acts of other Novo Nordisk Entities outside the EEA and to pay compensation for any damages resulting from the violation of the BCR by Novo Nordisk Entities.

If a non-EEA Novo Nordisk Entity is no longer a party to the BCR or otherwise ceases to exist, the third-party beneficiary rights provided to Data Subjects under this clause 1.5 will survive in order to ensure that the Data Subject's rights are not affected by such withdrawal from the BCR.

1.6 Novo Nordisk Data Protection Organization

Novo Nordisk A/S has appointed a global DPO for the Novo Nordisk group. The DPO has a Data Protection Office, which, together with the DPO, is responsible for overseeing compliance with the BCRs and ensuring that changes to the BCRs are notified to Novo Nordisk Entities covered by the BCR, to the European Supervisory Authorities and to data subjects who benefit from the BCR.

The Novo Nordisk Data Protection Office is supported by Data Protection Responsibles ("DPRs") and legal and compliance organizations at both regional and country levels,

who are responsible for ensuring compliance with the BCRs on a day-to-day basis. The DPO and the Novo Nordisk Data Protection Office reports to Novo Nordisk A/S' Executive Management and Board of Directors to ensure that senior management is committed to data protection in Novo Nordisk and to compliance with the BCRs.

1.7 Contact details

Questions regarding the provisions of the BCRs, data subject rights under the BCRs, or any other personal data protection issues, may be directed to the Novo Nordisk Data Protection Office:

Data Protection Office
+45 4444 8888
privacy@novonordisk.com
Novo Nordisk A/S
Krogshøjvej 55
2880 Bagsvaerd
Denmark

2 SUBSTANIVE PRINCIPLES FOR PROCESSING PERSONAL DATA

2.1 Compliance with local law

Novo Nordisk is committed to ensuring compliance with all applicable European Data Protection Laws and will ensure that where Personal Data is collected and processed, this is done in accordance with local law.

Where there is no law or the law in non-European countries does not meet the standards set out in the BCRs, Novo Nordisk will process Personal Data in compliance with the BCRs.

If there is reason to believe that local legislation applicable to any Novo Nordisk Entity prevents it from fulfilling its obligations under the BCR or such legislation has a substantial effect on its ability to comply with the BCR, Novo Nordisk will comply with the procedures set out in clause 4.3 below.

2.2 Lawfulness, fairness, and transparency

The processing of Personal Data by Novo Nordisk must be lawful, fair, and transparent to the data subject. Novo Nordisk will explain to data subjects about the processing of their Personal Data in accordance with clause 2.3 and will only obtain and process Personal Data for specified, explicit and legitimate purposes.

2.2.1 Lawfulness

The processing of Personal Data by Novo Nordisk shall be done lawfully in compliance with the relevant statutory provisions and with due regard for the principles laid down in the BCR.

The processing of Personal Data by a Novo Nordisk Entity is only permissible if at least one of the following prerequisites are fulfilled:

- the data subject has given his or her Consent;
- processing 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 to establish a contractual relationship with the data subject;
- processing is necessary to safeguard 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; or
- processing is necessary for compliance with the law of the Member State to which the controller is subject; or

- processing is necessary to protect the vital interests of the data subject or of another natural person.

2.2.2 Fairness (processing of Personal Data for new purposes)

Novo Nordisk will ensure that Personal Data is processed exclusively for specified, explicit, and legitimate purposes and that data subjects are informed about those purposes in accordance with clause 2.3.

Novo Nordisk will ensure that no processing of Personal Data is incompatible with the purposes for which the Personal Data were initially collected.

Using Personal Data for new or different purposes is only permitted if the data subject has given his/her Consent or if this is permitted under European Data Protection Laws, e.g., in the interest of scientific or historical research, and where Novo Nordisk have otherwise observed the requirements of the GDPR.

Novo Nordisk will ensure that data subjects are provided with information prior to such further processing on the purpose of such processing along with any other relevant information pursuant to clause 2.3 below, unless:

- the further processing is compatible with the purposes for which the Personal Data were initially collected; or

- Novo Nordisk has a legal basis for not doing so, as described in clause 2.3 below.

2.2.3 Transparency

Any processing of Personal Data by Novo Nordisk must be transparent for the data subject. Novo Nordisk will ensure that data subjects are provided with information as set out in articles 13 and 14 of the GDPR within the timelines for providing information set out herein. Novo Nordisk will ensure that the information provided is concise, easily accessible, and easy to understand, and that clear and plain language is used. Where appropriate, Novo Nordisk will use visualization to provide the information.

Novo Nordisk commits to make the BCR readily available to every data subject and the BCR will be available on Novo Nordisk's website and intranet.

2.3 Information to be provided to data subjects

Prior to processing any Personal Data on data subjects, it must be ensured that the data subject is provided with the information required pursuant to articles 13 and 14 of the GDPR.

When providing the information, Novo Nordisk will ensure to observe the requirements set out in this clause **Error! Reference source not found.**.

2.3.1 Personal Data obtained from the data subject

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

- the identity and contact details of the controller and its representative, if any;
- the contact details of Novo Nordisk's Data Protection Office;
- the purpose(s) of the processing and the legal basis for the processing;
- where the processing is based on a balancing of interests, the legitimate interest pursued by the relevant Novo Nordisk Entity;
- the recipients or categories of recipients;
- where applicable that the Personal Data is intended to be transferred to a third country, including how adequate safeguards for the protection of data is ensured and the means by which to obtain a copy of or more information on such adequate safeguards;

In addition, each Novo Nordisk Entity subject to the BCR will provide the following information to the data subject at the time when the Personal Data is obtained, insofar as such information is relevant and necessary to ensure fair and transparent processing:

- the period for which the Personal Data will be stored or if that is not possible, the criteria used to determine that period;
- the existence of the right to request 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;
- where a processing is based on consent, the right to withdraw such consent;

- the right to lodge a complaint with a Supervisory Authority;

- whether the voluntary 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

- whether automated decision-making, including profiling, 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 a Novo Nordisk Entity intends to process Personal Data for a different purpose than that for which the Personal Data were initially 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 the above.

2.3.2 Personal Data obtained from a third party

Where the Personal 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:

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

- the contact details of Novo Nordisk's Data Protection Office;

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

- the categories of Personal Data concerned;

- the recipients or categories of recipients;

- where applicable that the Personal Data is intended to be transferred to a third country, including how adequate safeguards for the protection of data is ensured and the means by which to obtain a copy of or more information on such adequate 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:

- the period for which the Personal Data will be stored or if that is not possible, the criteria used to determine that period;

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

- 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;

- where a processing is based on consent, the right to withdraw such consent;

- the right to lodge a complaint with a Supervisory Authority;

- from which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources;

- whether automated decision-making, including profiling, 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 a Novo Nordisk Entity intends to process Personal Data for a different purpose than that for which the Personal Data were initially 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 the above.

2.3.2.1 Timeline for providing information

Each Novo Nordisk Entity subject to the BCR will provide the information set out in this clause 2.3.2:

- within a reasonable period after obtaining the Personal Data, but no later than within one (1) month;

- 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 the data subject;

- if disclosure to a third party is envisaged, at the latest when the Personal Data is first disclosed to such third party.

2.3.2.2 Exceptions to providing data subjects with information

When provided for by applicable law of a Member State, data subjects, whose personal data are obtained from a third party, will not have a right to information under the following circumstances:

- 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 the conditions and safeguards referred to in article 89(1) of the GDPR, or in so far as the obligation referred to in this clause **Error! Reference source not found.** is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the relevant Novo Nordisk Entity will take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

- 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; or

- where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by EU or Member State law.

2.4 Accuracy and data minimization

Novo Nordisk will ensure that the Personal Data it processes is adequate, relevant and not excessive and will keep Personal Data accurate and up to date.

Data processing shall be guided by the principle of proportionality. The objective is to collect, process, and use only such Personal Data as is required for the relevant purpose of the processing. In particular, Novo Nordisk Entities will make use of the possibility to anonymize or pseudonymize Personal Data, provided that the cost and effort involved corresponds with the desired purpose. Statistical evaluations or studies based on anonymized Personal Data are not relevant for data protection purposes, provided that such Personal Data cannot be used to identify the data subject and provided that local law does not stipulate a higher level of protection for anonymized Personal Data than the BCR.

If Novo Nordisk learns that the Personal Data it processes is inaccurate or incomplete, Novo Nordisk will take appropriate measures to correct, block, or erase the data as relevant. Novo Nordisk actively encourages data subjects to inform Novo Nordisk when their Personal Data changes.

2.5 Storage limitation

Novo Nordisk will only keep Personal Data for as long as it is necessary for the purposes for which the Personal Data were originally collected.

Novo Nordisk has in place procedures (as amended from time to time) that set out principles and rules for data retention and which apply to all Novo Nordisk Entities subject to these BCRs. Novo Nordisk will ensure that these data retention requirements are aligned with the requirements and standards for data retention set out in applicable European Data Protection Laws.

Personal data that is no longer required for the purposes for which it was collected and stored will be destroyed, deleted, or anonymized, unless Novo Nordisk is prevented from doing so under applicable laws. In the event that statutory retention periods apply but the purpose of processing the Personal Data has been fulfilled, the data shall be blocked rather than erased.

2.6 Safeguarding the use of special Categories of Personal Data

Novo Nordisk may, if required for the purpose of the relevant processing activity, process and transfer Special Categories of Personal Data, namely health information about patients, clinical trial data and information on work related incidents.

Particular precaution must be taken if Special Categories of Personal Data are processed.

Should the processing of Special Categories of Personal Data be required, the explicit Consent of the data subject must be obtained, unless such processing is expressly permitted by the laws of a Member State (e.g., for the purpose of registering/protecting minorities), and additional requirements set out in the GDPR are complied with for the processing of Special Categories of Personal Data, including adequate security measures applicable for the processing of such Personal Data. Novo Nordisk Entities will not process on the basis of explicit consent under this clause 2.6, where EU or Member State law provide that the prohibition to process Special Categories of Personal Data referred to in article 9(1) of the GDPR may not be lifted by the data subject.

2.7 Data Security

Novo Nordisk has established and documented an IT security organization and has integrated data security into the processes of the organization.

Novo Nordisk Entities subject to the BCRs will always adhere to Novo Nordisk's IT security policies (as amended from time to time) and to any other data security procedures relevant to specific business areas or functions.

The Novo Nordisk Entities will take appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration,

unauthorized disclosure of or access to Personal Data transmitted, stored, or otherwise processed. Considering the state of the art and the costs of implementation, Novo Nordisk will ensure that such measures provide for a level of security appropriate to the risks represented by the processing and the nature of Personal Data (privacy by design). Such measures will further ensure that, by default, only Personal Data which are necessary for each specific purpose of the processing are processed (privacy by default).

Special Categories of Personal Data will be subject to specific security and protection measures.

Novo Nordisk has implemented a Personal Data Breach Response Process that sets out how all potential data breaches must be reported to Novo Nordisk's Data Protection Office and procedures for how the Data Protection Office and the Novo Nordisk Entities must handle personal data breaches. The Personal Data Breach Response Process also sets out how Novo Nordisk will ensure to notify relevant Supervisory Authorities without undue delay and no later than 72 hours after having become aware of a personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Further, the Personal Data Breach Response Process sets out how Novo Nordisk will ensure to notify data subjects 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.

Furthermore, 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 Supervisory Authorities on request.

Personal data breaches can be reported to Novo Nordisk via the internal Compliance Hotline or at privacy@novonordisk.com.

2.8 Direct marketing

Novo Nordisk Entities will ensure that any direct marketing activities are performed in compliance with applicable local EU Member State law.

The Novo Nordisk Entities will inform the data subjects on their right to object to the processing of the data subjects' Personal Data for advertising purposes or for purposes of market research and/or opinion polling purposes. The Novo Nordisk Entities will inform the data subject of its right to object free of charge to the processing of the data subject's Personal Data. In such cases, the Novo Nordisk Entities will refrain from contacting the data subjects who have opted out of receiving marketing information.

2.9 Use of data processors

If an external service provider to a Novo Nordisk Entity has access to Personal Data about data subjects (e.g., an external hosting provider), the following requirements will be observed:

- the service provider is assessed and selected by the Novo Nordisk Entity being the controller on the basis of the processor's ability to ensure the implementation and maintenance of necessary technical and organizational security measures required for complying with the Novo Nordisk BCR in relation to data processing;
- the controller will ensure and regularly verify that the processor remains fully compliant with the agreed technical and organizational security requirements;
- the rights and obligations of the processor 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:
    - processes the Personal Data only on documented instructions from the controller;
    - ensures the confidentiality of persons processing the Personal Data;
    - will not engage another processor without prior authorisation from the controller;
    - takes all measures required to implement the necessary technical and organisational security measures;
    - 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;
    - assists the controller with answering requests from data subjects to exercise their rights;
    - that the processor remains liable to the controller for any breach of the data protection obligations by a sub-processor;
    - assists the controller in ensuring compliance with applicable security requirements, notification of Supervisory Authorities and data subjects in case of a data breach and with conducting data protection impact assessments and prior consultations with Supervisory Authorities, if necessary;
    - at the choice of the controller deletes or returns all copies of the Personal Data to the controller upon termination of the services;

- makes available to the controller all information necessary to demonstrate compliance with data protection legislation, in particular that the processor will contribute to audits, including inspections, conducted by the controller or a third party appointed by the controller; and
- the controller retains responsibility for the legitimacy of the processing and continues to be the point of contact for the data subject.

Where Novo Nordisk Entities process Personal Data on behalf of other Novo Nordisk Entities, a written agreement must be entered between the Novo Nordisk Entities acting as processor and controller, respectively. Such agreement must meet the requirements set out in this clause 2.9.

2.10 Transfers to third parties outside Europe

Novo Nordisk Entities subject to the BCRs will not transfer Personal Data to a third party (i.e. a company that is not bound by the BCRs) outside Europe unless one of the following conditions are met:

- An adequacy decision by the EU Commission states that the country outside Europe has an adequate level of protection in accordance with Article 45 of the GDPR;
- The receiving entity demonstrates that it has an adequate level of protection for personal data within the meaning of Article 46 of the GDPR, e.g. by concluding EU Commission Standard Contractual Clauses or by concluding other appropriate contractual agreements between the transferring and the receiving entity, and provided that Novo Nordisk has assessed that the level of protection of the data subject's fundamental rights and freedoms is essentially equivalent to that guaranteed within the EU/EEA (in light of the Charter of Fundamental Rights in the EU) taking into account all circumstances of the transfer and any supplementary measures which may be necessary implement in order to safeguard the transfer; or
- Another valid legal basis under EU or Member State law has been established in accordance with chapter V of the GDPR.

A transfer may, under limited circumstances, be permissible under the derogations defined in Article 49 of the GDPR to the extent such transfer is not massive, disproportionate, or indiscriminate.

2.11 Accountability

Everyone who works for or on behalf of Novo Nordisk is:

- responsible and accountable for processing Personal Data ethically and lawfully and in compliance with the provisions of the BCR and applicable Data Protection Laws;
- expected to comply with Novo Nordisk policies and procedures when processing Personal Data.

Novo Nordisk has processes and procedures in place to manage and oversee our compliance with data protection requirements, including the BCR. Further, Novo Nordisk has appropriate technical and organizational measures in place to enable compliance with these requirements. Everyone at Novo Nordisk is expected to follow Novo Nordisk's processes and comply with Novo Nordisk's procedures relevant to processing of Personal Data.

3 RIGHTS OF THE DATA SUBJECT

3.1 Respect for data subjects' rights

Each Novo Nordisk Entity subject to the BCR will adhere to the Data Subject's Requests and Complaint Handling Procedure set out in Appendix 1 and will be receptive to any queries or requests made by data subjects regarding the processing of their Personal Data.

Each Novo Nordisk Entity will ensure that all data subjects will be able to obtain:

- confirmation as to whether or not Personal Data relating to the data subjects is being processed and at least the following information:
    - the purposes of the processing,
    - the categories of Personal Data concerned,
    - the recipients or categories of recipients to whom the Personal Data are disclosed,
    - the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period,
    - the existence of the right to request from the Novo Nordisk Entity rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the data subject or to object to such processing,
    - the right to lodge a complaint with a Supervisory Authority,

- where the Personal Data are not collected from the data subject, any available information as to their source, and
- whether automated decision making, including profiling, 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;

- communication to the data subject in an intelligible form of the Personal Data undergoing processing and of any available information as to their source, including a copy of the Personal Data undergoing processing;
- the rectification, erasure or blocking 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;
- notification to third parties to whom the data has been disclosed of any rectification, erasure or blocking carried out in compliance with the above, unless this proves impossible or involves a disproportionate effort, without constraint, at reasonable intervals and without excessive delay or expense;
- restriction of a Novo Nordisk Entity's processing of the data subject's Personal Data where:
    - 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;
    - the processing is unlawful, and the data subject opposes the erasure of the Personal Data and requests the restriction of their use instead;
    - 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;
- the right to request portability of Personal Data, which the data subject has provided to Novo Nordisk, where the processing by Novo Nordisk is based on Consent or on a contract with the data subject and where the processing is carried out by automated means.

- 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 a balancing of interests, including profiling based on the balancing of interests.
- 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.

The law of a Member State may restrict the data subject's rights set out above, including the right to access if this right is exercised repeatedly within a short period of time, unless the data subject can show a legitimate reason for the repeated assertion of claims for information. Further, Novo Nordisk may restrict the data subject's right to access if the right adversely affects the rights and freedoms of others.

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 charge a reasonable fee, considering the administrative costs of providing the information or communication or taking the action requested, for providing the information set out above.

Further, each Novo Nordisk Entity will ensure that all data subjects may at any time object to Novo Nordisk's processing of data relating to the data subject. Where the objection is justified, each Novo Nordisk Entity will ensure that the Personal Data is erased and will no longer undergo processing.

The data subject can assert the above rights by contacting Novo Nordisk's Data Protection Office at privacy@novonordisk.com.

3.2 Record of processing activities and Data Protection Impact Assessment

Novo Nordisk has established and maintains a record of all categories of processing activities carried out by Novo Nordisk that are subject to the BCR. The record of processing activities contains the information set out in article 30 of the GDPR.

The record is maintained in writing, including in electronic form, and will be made available to a Supervisory Authority on request.

Novo Nordisk will assess the risk of its processing activities subject to the BCR and where it is assessed that a processing activity is likely to result in a high risk to the rights and freedoms of natural persons, Novo Nordisk will in cooperation with the local DPR carry out a data protection impact assessment in accordance with Article 35 of the GDPR.

If the data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by Novo Nordisk to mitigate the risk, the local DPR must consult the Novo Nordisk Data Protection Office, who will consult the competent Supervisory Authority, prior to processing Personal Data for the relevant processing activity.

3.3 Automated decision-making

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. Decisions which have legal consequences for the data subject or substantially prejudice the data subject may not be reached exclusively on the basis of an automated individual procedure designed to evaluate an individual's personal characteristics. An exception applies only if the decision:

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

Where the decision is based on the entering into or performance of a contract or the data subjects' explicit consent, the Novo Nordisk Entities will ensure to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. This includes implementing the right to obtain human intervention with the Novo Nordisk Entity, to express his or her point of view and to contest the decision.

4 NOVO NORDISK COMMITMENTS

4.1 Training

Novo Nordisk will provide appropriate training to employees who regularly process Personal Data or are involved in the development of tools used to process Personal Data.

All relevant employees and contractors are provided training on personal data protection (including the principles in these BCRs) through e-learning, guidelines, policies, and face-to-face training sessions by the Novo Nordisk Data Protection Office, DPRs, and local legal and compliance organizations on an annual basis or ad hoc as needed.

4.2 Relationship between BCR and local statutory regulations

The legitimacy of the processing of Personal Data is judged on the basis of the applicable local law. To the extent that the applicable local law stipulates a higher level of protection of Personal Data than the BCR, data processing shall be in accordance with the applicable law. Each Novo Nordisk Entity shall check for itself, whether local data protection laws exist and shall ensure compliance with these. If the applicable local law provides a lower level of protection for Personal Data than the BCR, the present BCR shall be applied.

4.3 Actions in case of legislation preventing compliance with BCRs

4.3.1 **Obligations prior to Transfers of Personal Data**
Any Novo Nordisk Entity transferring Personal Data out of the EU/EEA will, with help from the recipient, and taking into account the circumstances of the transfer, evaluate prior to the transfer if national legislation will prevent the Novo Nordisk Entity from fulfilling its obligations under these BCRs. In addition, the Novo Nordisk Entity will determine any required supplementary measures to be taken in accordance with section 4.3.3 below. The Novo Nordisk DPO will review and approve the evaluation and any proposed supplementary measures.

4.3.2 **Obligations where a Transfer of Personal Data already takes place**
Where a Novo Nordisk Entity already transfers Personal Data out of the EU/EEA and national legislation is amended or otherwise updated, the Novo Nordisk Entity will, before the amended or updated national legislation enters into force, and with help from the recipient, evaluate if the amended or otherwise updated national legislation will prevent the Novo Nordisk Entity from fulfilling its obligations under these BCRs. In addition, the Novo Nordisk Entity will determine required supplementary measures to be taken in accordance with section 4.3.3 below. The Novo Nordisk DPO will review and approve the evaluation and any proposed supplementary measures.

4.3.3 **Supplementary measures**
Where the evaluation of national legislation in accordance with section 4.3.1 and 4.3.2 of these BCRs requires supplementary measures, Novo Nordisk will implement the required supplementary measures. The Novo Nordisk DPO will review and approve any proposed supplementary measures. If no sufficient supplementary measures can be put in place, the Novo Nordisk Entity must suspend the transfer immediately and, if the transfer does already take place, the recipient must return the transferred Personal Data to the Novo Nordisk Entity and delete any existing copies.

4.3.4 **National legislation which requires a higher level of protection**
Where national legislation requires a higher level of protection of Personal Data than what is established under these BCRs, national legislation shall prevail, and Novo Nordisk shall process Personal Data in accordance with the national legislation.

4.3.5 **Documentation**
The outcome of any evaluations carried out in accordance with section 4.3.1 and 4.3.2 of these BCRs and any proposed supplementary measures will be documented and made available to the relevant European Supervisory Authority on request.

4.3.6 **Notification in case of conflicts between national legislation and the BCRs**

If a Novo Nordisk Entity has reasons to believe that the existing or future national legislation applicable to it may prevent it from fulfilling the instructions received from the Novo Nordisk Entity acting as data controller or its obligations under the BCRs, it

will promptly consult the Novo Nordisk DPO and notify this to the Novo Nordisk Entity acting as data controller, which is entitled to suspend the transfer of Personal Data, to the Novo Nordisk Entity acting as data processor, EU member with delegated data protection responsibilities, but also to the European Supervisory Authority competent for the Novo Nordisk Entity acting as controller and the European Supervisory Authority competent for the Novo Nordisk Entity acting as data processor.

4.3.7 **Legally binding requests for disclosure of Personal Data**

4.3.7.1 Any legally binding request for disclosure of the Personal Data by a law enforcement authority or state security body shall be communicated to the Novo Nordisk Entity acting as data controller unless otherwise prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). In any case, the request for disclosure should be put on hold and the competent European Supervisory Authority for the Novo Nordisk Entity acting as data controller and the Novo Nordisk Entity acting as data processor should be clearly informed about the request, including information about the Personal Data requested, the requesting body and the legal basis for disclosure (unless otherwise prohibited).

4.3.7.2 If in specific cases the suspension and/or notification are prohibited, the BCRs shall provide that the requested Novo Nordisk Entity will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible and be able to demonstrate that it did so.

4.3.7.3 If, in the above cases, despite having used its best efforts, the requested Novo Nordisk Entity is not in a position to notify the competent European Supervisory Authority, it must commit in the BCRs to annually provide general information on the requests it received to the competent European Supervisory Authority (e.g., number of applications for disclosure, type of Personal Data requested, requester if possible, etc.).

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

4.3.8 Transfers and disclosures not authorised by EU/EEA law, whether by a court or a tribunal, and any decision of an administrative authority of a country outside the EU/EEA which requires a Novo Nordisk Entity to transfer or disclose Personal Data to a country outside the EU/EEA shall only be recognised or enforceable in any way if the judgment or decision is based on an international agreement, e.g. mutual legal assistance treaty, which is in force between the country outside the EU/EEA in question and the EU/EEA or EU/EEA member state, without prejudice to other grounds for transfer of Personal Data pursuant to Chapter V of the GDPR.

4.4 Audit

Novo Nordisk will comply with the BCR Audit Protocol in Appendix 2 to verify compliance with the BCRs and ensure corrective actions to protect data subject rights.

4.5 Complaint handling

Novo Nordisk will comply with the Data Subject's Requests and Complaint Handling Procedure in Appendix 1.

4.6 Cooperation with European Supervisory Authorities

Novo Nordisk will comply with the Cooperation Procedure in Appendix 3.

4.7 Update of the BCR

Novo Nordisk will comply with the BCR Updating Procedure in Appendix 4.

APPENDIX 1 DATA SUBJECT'S REQUESTS AND COMPLAINT HANDLING PROCEDURE

1. BACKGROUND

The GDPR gives data subjects whose Personal Data is collected and/or processed and used in the EEA certain rights. This procedure explains how Novo Nordisk deals with the following rights of the data subject:

- **Right of access.** The right to obtain confirmation as to whether or not Personal Data concerning the data subject are being processed, and where that is the case, access to the information and in addition certain information as set out below (also known as an "access request").

- **Right to rectification.** The right to request rectification of inaccurate Personal Data concerning him or her, including the right to have incomplete Personal Data completed.

- **Right to erasure.** The right to request erasure of Personal Data concerning him or her.

- **Right to restriction of processing.** The right to request restriction of processing of Personal Data concerning him or her.

- **Right to data portability.** The right to request portability of Personal Data, which the data subject has provided to Novo Nordisk, where the processing by Novo Nordisk is based on Consent or on a contract with the data subject and where the processing is carried out by automated means.

- **Right to object.** The right to at any time object to the processing of Personal Data concerning him or her, 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, which produces legal affects or significantly affects the data subject, and against receiving direct marketing material.

- **Right to complain to Novo Nordisk and/or Supervisory Authorities.** The right to complain to Novo Nordisk or a competent Supervisory Authority regarding the processing of the data subjects Personal Data by a Novo Nordisk Entity. This includes complaints regarding the response to a data subject request by Novo Nordisk Entities as well as complaints about Novo Nordisk's compliance with the BCR.

2. HOW TO MAKE A REQUEST OR COMPLAINT

Data subjects whose Personal Data is processed by Novo Nordisk under these BCRs can make a request or bring a complaint by contacting the Novo Nordisk Data Protection Office:

privacy@novonordisk.com
+45 4444 8888
Novo Nordisk A/S
Krogshøjvej 55
2880 Bagsvaerd
Denmark

3. PROCEDURE FOR RECEIPT OF REQUESTS AND COMPLAINTS

The Novo Nordisk Data Protection Office handles data subject requests and complaints arising under the BCRs in coordination with Local Data Protection Responsibles and local legal and compliance functions.

If any employee or subcontractor of a Novo Nordisk Entity receives any request or complaint from a data subject, they must pass the request to the Local Data Protection Responsible and the Data Protection Office immediately upon receipt indicating the date on which the request or complaint was received together with any other information which may assist the Local Data Protection Responsible and Data Protection Office to deal with the request or complaint.

The request or complaint does not have to be official or mention data protection law to qualify as a data subject request or complaint.

3.1 Relevant information from a data subject

The data subject making a request or bringing a complaint must provide proof of identity before the request can be processed by the relevant Novo Nordisk Entity.

Under normal circumstances no fee will be applied by the Novo Nordisk Entities for the processing of the request or complaint.

Novo Nordisk may ask for such information that it may reasonably require to confirm the identity of the data subject making the request or bringing the complaint and to locate the Personal Data, which the data subject seeks, however failure to provide information to locate the Personal Data shall not result in a refusal of a request.

3.2 Initial assessment of all requests and complaints

The Data Protection Office in coordination with the Local Data Protection Responsible will make an initial assessment of the request or complaint 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.

The Local Data Protection Responsible will then contact the data subject in writing to confirm receipt of the request or complaint, seek confirmation of identity or further information, if required, or decline the request or complaint if one of the exemptions set out under section 4.2 of this Appendix 1 applies. Where Novo Nordisk cannot comply with the request or complaint, Novo Nordisk will inform the data subject accordingly.

4. ACCESS REQUESTS

4.1 Approach and scope

A data subject making an access request to a Novo Nordisk Entity under this procedure is entitled to:

- Be informed whether the Novo Nordisk Entity holds and is processing Personal Data about that data subject.
- Be given at least the following information:
    - the purposes of the processing,
    - the categories of Personal Data concerned,
    - the recipients or categories of recipients to whom the Personal Data are disclosed,
    - the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period,
    - the existence of the right to request from the Novo Nordisk Entity rectification or erasure of Personal Data or restriction of processing of Personal Data concerning the data subject or to object to such processing,
    - the right to lodge a complaint with a Supervisory Authority,
    - where the Personal Data are not collected from the data subject, any available information as to their source, and
    - whether automated decision making, including profiling, 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.

- Communication in intelligible form of the Personal Data held by the Novo Nordisk Entity.

4.2 Exemptions to subject access

An access request may be refused where the access request is made to a European Novo Nordisk Entity and relates to Personal Data controlled by that entity, if the refusal to provide the information is consistent with the law of the Member State in which the Novo Nordisk Entity is established.

4.3 The search and the response

The Novo Nordisk Data Protection Office, or a Local Data Protection Responsible will arrange a search of relevant electronic and paper filing systems.

The Personal Data requested will be collated by the Data Protection Office/Local Data Protection Responsible 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 Protection Office/Local Data Protection Responsible which includes information required to be provided in response to a request.

Where the provision of the information in permanent form is not possible or in cases where the interests of the data subject speak in favor thereof 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 Protection Office/Local Data Protection Responsible or to receive the information in another form.

5. OTHER REQUESTS

If a request is received for erasure, restriction of processing or portability of a data subject's Personal Data, or if a data subject objects to the processing of his or her Personal Data by Novo Nordisk, such a request must be considered and dealt with as appropriate by the Data Protection Office in coordination with the Local Data Protection Responsible.

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 a Novo Nordisk Entity is satisfied that there is a legitimate basis for doing so.

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 referred by the Local Data Protection Responsible to the Novo Nordisk Data Protection Office to assess. 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.

6. COMPLAINT HANDLING

The Novo Nordisk Data Protection Office handles all complaints arising under the BCRs in coordination with Local Data Protection Responsibles and local legal and compliance functions. The Novo Nordisk Data Protection Office will handle the complaint in a diligent and efficient manner and will 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. Novo Nordisk Data Protection Office will liaise with colleagues from relevant business and support units as appropriate to deal with complaints.

6.1 Disputing a finding

If the data subject is not satisfied with the way in which the complaint has been resolved, data subjects have rights under the BCR to complain to a European Supervisory Authority and/or lodge an application with a court of competent jurisdiction to enforce the third-party beneficiary rights set out in section 6.2 below.

Individuals entitled to such rights will be notified accordingly as part of the complaint handling procedure and will 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 a European 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.

6.2 Third party beneficiary rights

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 be able to enforce the following third-party beneficiary rights against such Novo Nordisk Entity:

- **Enforce compliance.** Seek enforcement of compliance with these BCRs, including its appendices, including but not limited to seeking enforcement of the following rights and principles:
    - The substantive principles for the processing of Personal Data set out in clause 2;
    - The rights of the data subject set out in clause 3;
    - Local statutory regulations insofar as such local law stipulates a higher level of protection of Personal Data than the BCR;
    - The right to make a complaint through the procedure set out in the Data Subjects' Requests Procedure;
    - Any support of or cooperation needed with European Supervisory Authorities.

- **Complain to Novo Nordisk.** Complain to a Novo Nordisk Entity established in Europe responsible for exporting the Personal Data in accordance with this Data Subject's Requests and Complaint Handling Procedure, and seek appropriate redress from the Novo Nordisk Entity in Europe responsible for exporting the Personal Data including the remedy of any breach of the BCR by the non-European Novo Nordisk Entity.

- **Seek compensation.** To obtain redress and where appropriate, receive compensation from the Novo Nordisk Entity responsible for exporting the Personal Data or the Novo Nordisk Headquarters for any damage suffered as a result of a breach of the BCR by the non-European Novo Nordisk Entity importing the Personal Data.

- **Complain to a European Supervisory Authority.** Lodge a complaint with a European Supervisory Authority of competent jurisdiction as regards the exporting Novo Nordisk Entity, in particular in the Member State of the data subject's;
    - habitual residence;
    - place of work; or
    - where the alleged infringement of the BCR occurred; and/or.

- **Take judicial action.** Take action against a Novo Nordisk Entity in order to enforce compliance with the BCR in the courts of the jurisdiction in which the European Novo Nordisk Entity responsible for exporting the Personal Data to a Novo Nordisk Entity established in a non-European country is established or in the courts of the jurisdiction in which the data subject has his or her habitual residence either against the European Novo Nordisk Entity responsible for exporting the Personal Data or against the Novo Nordisk Entity established in a non-European country importing the Personal Data in order to enforce compliance with the BCR, including the appendices.

- **Copy of the BCR.** Obtain a copy of the BCR with its appendices and the Unilateral Declaration on request or by obtaining a copy of the BCR on Novo Nordisk's website.

Novo Nordisk agrees that the burden of proof to show that a Novo Nordisk Entity outside Europe is not responsible for the breach, or that no such breach took place, will rest with the European Novo Nordisk Entity responsible for exporting the Personal Data to a Novo Nordisk Entity outside Europe. For claims directed towards the Novo Nordisk Headquarter, the burden of proof will be on the Novo Nordisk Headquarter, regardless of which Novo Nordisk entity was responsible for the alleged breach.

In addition, claims may be brought against the Novo Nordisk Headquarters, which has undertaken to accept responsibility for and agreed to take the necessary action to remedy the acts of other Novo Nordisk Entities outside the EEA and to pay compensation for any damages resulting from the violation of the BCR by Novo Nordisk Entities.

In the event that a non-EEA Novo Nordisk Entity is no longer a party to the BCR or otherwise ceases to exist, the third-party beneficiary rights provided to Data Subjects under this clause 6.2 will survive in order to ensure that the Data Subject's rights are not affected by such withdrawal from the BCR.

7. TIMELINE FOR RESPONDING TO A REQUEST OR COMPLAINT

Subject to the data subject providing proof of identity and residence, a Novo Nordisk Entity must respond to a request or complaint without undue delay and in any event within one (1) month of receipt of the request or complaint. The period for responding to the request may be extended by two (2) further months where necessary, taking into account the complexity and number of requests. The Data Protection Office/Local Data Protection Responsible will inform the data subject of any such extension within one (1) month of receipt of the request or complaint, together with the reasons for the delay.

8. FURTHER INFORMATION AND REVIEW OF PROCEDURE

If any more information about this procedure or any other aspect of subject access is needed, please contact:

Data Protection Officer
+45 4444 8888
privacy@novonordisk.com
Novo Nordisk A/S
Krogshøjvej 55
2880 Bagsvaerd
Denmark

This Procedure will be reviewed and considered in line with applicable EU and Member State laws and case law on subjects' access cases and subject to procedures under the BCRs.

APPENDIX 2 BCR AUDIT PROTOCOL

1. Background
To verify compliance with the BCRs, Novo Nordisk's Group Internal Audit function ("GIA") will be responsible for carrying out data protection audits. From time to time, Novo Nordisk may appoint other internal functions or accredited third party auditors to carry out the audits on its behalf. GIA will manage and provide quality assurance of audit work performed by third parties.

2. Scope and timing of audit
GIA will ensure that such audits address all aspects of the BCRs, including relevant IT systems, databases, policies, training, and contractual provisions in place within Novo Nordisk. GIA will decide the scope of audits based on a risk and materiality assessment that is updated annually. GIA will conduct at least one audit of the BCRs each year.

3. Responsibility for compliance
GIA will be responsible for bringing the result of an audit to the attention of Novo Nordisk's DPO, Novo Nordisk A/S' Executive Management and Board of Directors, who are all committed to ensuring that any corrective actions remedying any non-compliance will take place as soon as is reasonably possible.

4. Cooperation with European Supervisory Authorities
Novo Nordisk agrees to provide results of any audit of the BCRs to a European Supervisory Authority of competent jurisdiction upon request subject to applicable law. GIA will be responsible for liaising with the European Supervisory Authorities for this purpose.

In addition, Novo Nordisk agrees that European Supervisory Authorities may audit Novo Nordisk Entities to review compliance with the BCRs in accordance with the provisions of the Cooperation Procedure in Appendix 3. The Novo Nordisk Data Protection Office and GIA will be responsible for liaising with the European Supervisory Authorities for this purpose.

APPENDIX 3 CO-OPERATION PROCEDURE

This Data Protection Binding Corporate Rules Co-operation Procedure sets out the way in which Novo Nordisk will co-operate with the European Supervisory Authorities in relation to the BCR.

Where required, Novo Nordisk will make the necessary personnel available for dialogue with a European Supervisory Authority in relation to the BCRs.

Novo Nordisk will abide by:

- Advice given by the relevant European Supervisory Authority on any data protection law issues that may affect the interpretation and application of the BCRs; and

- The views of the European Data Protection Board (EDPB) as outlined in its published guidance on Binding Corporate Rules.

Novo Nordisk will provide, upon request, the results of any audit of the BCRs to a European Supervisory Authority of competent jurisdiction subject to applicable law.

Where a Novo Nordisk Entity is located within the jurisdiction of a Supervisory Authority based in Europe, Novo Nordisk agrees that that the Supervisory Authority may audit that Novo Nordisk Entity for the purpose of reviewing compliance with the BCRs, in accordance with the applicable law of the country in which the Novo Nordisk Entity is located, or, in the case of a Novo Nordisk Entity located outside Europe, in accordance with the applicable law of the European country from which the Personal Data is transferred under the BCR.

Novo Nordisk agrees to abide by a decision of the relevant European Supervisory Authority on any issues related to the interpretation and application of the BCRs.

APPENDIX 4 BCR UPDATING PROCEDURE

This BCR Updating Procedure sets out the way in which Novo Nordisk will communicate changes to the BCR to the relevant EEA Supervisory Authorities, data subjects and to the Novo Nordisk Entities bound by the BCR.

The Novo Nordisk Data Protection Office will keep track of and record any updates to the BCR and provide the necessary information to the data subjects or European Supervisory Authorities upon request.

Novo Nordisk Data Protection Office will without undue delay communicate any material revisions to the BCRs to the Danish Data Protection Agency, and any other relevant European Supervisory Authorities as required, including revisions due to change of applicable Data Protection Law in any European country, through any legislative, court or Supervisory Authority measure. The Novo Nordisk Data Protection Office will also provide a brief explanation of the reasons for any notified changes to the BCR. Novo Nordisk will once a year provide the Danish Data Protection Agency with an overview of changes made, which are not considered to be substantial.

Where a modification would possibly affect the level of the protection offered by the BCRs or significantly affect the BCRs (i.e. changes to the binding character), such modifications will be promptly communicated to the Danish Data Protection Agency and any other relevant European Supervisory Authorities if required.

Novo Nordisk will communicate any changes to the BCRs to the Novo Nordisk Entities bound by the BCRs and to the data subjects who benefit from the BCRs. Novo Nordisk Data Protection Office will maintain a change log which sets out the date the BCRs is revised and the details of any revisions made.

The Novo Nordisk Data Protection Office will maintain an up-to-date list of Novo Nordisk Entities bound by these BCRs and ensure that all new Novo Nordisk Entities are bound by and can deliver compliance with the BCRs before a transfer of Personal Data to them takes place.

APPENDIX 5 OVERVIEW OF DATA PROCESSING ACTIVITIES COVERED BY THE BCR

Processing activities	Purpose of processing	Categories of data subjects	Categories of personal data	Categories of recipients (in scope of the BCR)	International transfer destination	Place of storage	Time limits for erasure
Human resources (HR)	Recruitment, Hiring, Personnel Administration, Performance Management, Employee Development and Exit of employees	Employees, applicants, former employees	Contact information, CVs, applications, employment details, performance details, health information, criminal records, union membership.	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, China and USA. Further, data may be transferred to the following international transfer destinations where Novo Nordisk Entities are established	For the centralized HR system, data is mainly stored within Denmark, Switzerland, India, China and USA. Data may also to a limited extent be stored to in the following countries where the Novo Nordisk Entities are established (subject to applicable law): Albania, Algeria, Australia, Azerbaijan,	Following local law requirements for keeping HR data and subject to clause 2.5 of the BCR.

					(subject to applicable law): Albania, Algeria, Australia, Azerbaijan, Bangladesh, Bosnia and Herzegovina, Brazil, Chile, China, Colombia, Ecuador, Egypt, Hong Kong, India, Indonesia, Iraq, Islamic Republic of Iran, Jordan, Kazakhstan, Kenya, Kosovo, Lebanon, Malaysia, Mexico, Montenegro, Morocco, Nigeria, Pakistan, Panama, Peru, Philippines,	Bangladesh, Bosnia and Herzegovina, Brazil, Chile, China, Colombia, Ecuador, Egypt, Hong Kong, India, Indonesia, Iraq, Islamic Republic of Iran, Jordan, Kazakhstan, Kenya, Kosovo, Lebanon, Malaysia, Mexico, Montenegro, Morocco, Nigeria, Pakistan, Panama, Peru, Philippines, Republic of Korea, Republic of Moldova, Russian Federation, Saudi Arabia, Serbia, Singapore, South Africa,	

					Republic of Korea, Republic of Moldova, Russian Federation, Saudi Arabia, Serbia, Singapore, South Africa, Sri Lanka, Syrian Arab Republic, Taiwan, Thailand, The Former Yugoslav Republic of Macedonia, Tunisia, Turkey, Ukraine, Ukraine, United Arab Emirates, Uzbekistan, Venezuela and Viet Nam.	Sri Lanka, Syrian Arab Republic, Taiwan, Thailand, The Former Yugoslav Republic of Macedonia, Tunisia, Turkey, Ukraine, Ukraine, United Arab Emirates, Uzbekistan, Venezuela and Viet Nam.	

Customer management	Management of customer relationships.	Customers, patients/users, HCPs	Contact information, customer relationship details	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, China and USA. Further, data may be transferred to the following international transfer destinations where Novo Nordisk Entities are established (subject to applicable law): Albania, Algeria, Australia,	For the centralized CRM system, data is mainly stored within Denmark, Switzerland, India, China and USA. Data may also to a limited extent be stored in the following countries where the Novo Nordisk Entities are established (subject to applicable law): Albania, Algeria, Australia, Azerbaijan, Bangladesh, Bosnia and Herzegovina, Brazil, Chile, China, Colombia, Ecuador, Egypt,	Following local law requirements for keeping CRM data and subject to clause 2.5 of the BCR.

					Azerbaijan, Bangladesh, Bosnia and Herzegovina, Brazil, Chile, China, Colombia, Ecuador, Egypt, Hong Kong, India, Indonesia, Iraq, Islamic Republic of Iran, Jordan, Kazakhstan, Kenya, Kosovo, Lebanon, Malaysia, Mexico, Montenegro, Morocco, Nigeria, Pakistan, Panama, Peru, Philippines, Republic of Korea, Republic of Moldova, Russian Federation, Saudi Arabia,	Hong Kong, India, Indonesia, Iraq, Islamic Republic of Iran, Jordan, Kazakhstan, Kenya, Kosovo, Lebanon, Malaysia, Mexico, Montenegro, Morocco, Nigeria, Pakistan, Panama, Peru, Philippines, Republic of Korea, Republic of Moldova, Russian Federation, Saudi Arabia, Serbia, Singapore, South Africa, Sri Lanka, Syrian Arab Republic, Taiwan, Thailand, The Former Yugoslav	

					Serbia, Singapore, South Africa, Sri Lanka, Syrian Arab Republic, Taiwan, Thailand, The Former Yugoslav Republic of Macedonia, Tunisia, Turkey, Ukraine, Ukraine, United Arab Emirates, Uzbekistan, Venezuela and Viet Nam.	Republic of Macedonia, Tunisia, Turkey, Ukraine, Ukraine, United Arab Emirates, Uzbekistan, Venezuela and Viet Nam.	

Supplier management-	Management of relationships with suppliers and other business contacts, including Health Care Professionals (HCPs)	Suppliers, other business contacts, including HCPs	Contact information, relationship details. Financial information.	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 and business support functions in India, China and USA. Further, data may be transferred to the following international transfer destinations where Novo Nordisk Entities are established (subject to applicable law): Albania, Algeria, Australia,	For the centralized ERP system, data is mainly stored in Ireland, India, China and USA. Data may also to a limited extent be stored in the following countries where the Novo Nordisk Entities are established (subject to applicable law): Albania, Algeria, Australia, Azerbaijan, Bangladesh, Bosnia and Herzegovina, Brazil, Chile, China, Colombia, Ecuador, Egypt, Hong Kong, India, Indonesia, Iraq,	Following local law requirements for keeping CRM data and subject to clause 2.5 of the BCR.

					Azerbaijan, Bangladesh, Bosnia and Herzegovina, Brazil, Chile, China, Colombia, Ecuador, Egypt, Hong Kong, India, Indonesia, Iraq, Islamic Republic of Iran, Jordan, Kazakhstan, Kenya, Kosovo, Lebanon, Malaysia, Mexico, Montenegro, Morocco, Nigeria, Pakistan, Panama, Peru, Philippines, Republic of Korea, Republic of Moldova, Russian Federation, Saudi Arabia,	Islamic Republic of Iran, Jordan, Kazakhstan, Kenya, Kosovo, Lebanon, Malaysia, Mexico, Montenegro, Morocco, Nigeria, Pakistan, Panama, Peru, Philippines, Republic of Korea, Republic of Moldova, Russian Federation, Saudi Arabia, Serbia, Singapore, South Africa, Sri Lanka, Syrian Arab Republic, Taiwan, Thailand, The Former Yugoslav Republic of Macedonia, Tunisia, Turkey,	

					Serbia, Singapore, South Africa, Sri Lanka, Syrian Arab Republic, Taiwan, Thailand, The Former Yugoslav Republic of Macedonia, Tunisia, Turkey, Ukraine, Ukraine, United Arab Emirates, Uzbekistan, Venezuela and Viet Nam.	Ukraine, Ukraine, United Arab Emirates, Uzbekistan, Venezuela and Viet Nam.	
Research, development and safety	Clinical research, product development and pharmacovigilance	Patients, HCPs, clinical trial investigators, suppliers	Contact information, relationship details, health related information (patients), biosamples.	Novo Nordisk Entities as defined in the BCR and as listed in Appendix 6.	Data is collected at local sites or local Novo Nordisk entities and transferred to Novo Nordisk A/S's corporate systems. Data may be	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

					shared with central functions in HQ in Denmark or regional HQ in Switzerland, and with business support functions in India, China and USA. Further, data may be transferred to the following international transfer destinations where Novo Nordisk Entities are established (subject to applicable law): Albania, Algeria, Australia, Azerbaijan,	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 stored in the following countries where the Novo Nordisk Entities are established (subject to applicable law): Albania, Algeria, Australia, Azerbaijan, Bangladesh, Bosnia and Herzegovina, Brazil, Chile, China, Colombia,	and subject to clause 2.5 of the BCR.

					Bangladesh, Bosnia and Herzegovina, Brazil, Chile, China, Colombia, Ecuador, Egypt, Hong Kong, India, Indonesia, Iraq, Islamic Republic of Iran, Jordan, Kazakhstan, Kenya, Kosovo, Lebanon, Malaysia, Mexico, Montenegro, Morocco, Nigeria, Pakistan, Panama, Peru, Philippines, Republic of Korea, Republic of Moldova, Russian Federation, Saudi Arabia, Serbia,	Ecuador, Egypt, Hong Kong, India, Indonesia, Iraq, Islamic Republic of Iran, Jordan, Kazakhstan, Kenya, Kosovo, Lebanon, Malaysia, Mexico, Montenegro, Morocco, Nigeria, Pakistan, Panama, Peru, Philippines, Republic of Korea, Republic of Moldova, Russian Federation, Saudi Arabia, Serbia, Singapore, South Africa, Sri Lanka, Syrian Arab Republic, Taiwan, Thailand, The Former	

					Singapore, South Africa, Sri Lanka, Syrian Arab Republic, Taiwan, Thailand, The Former Yugoslav Republic of Macedonia, Tunisia, Turkey, Ukraine, Ukraine, United Arab Emirates, Uzbekistan, Venezuela and Viet Nam.	Yugoslav Republic of Macedonia, Tunisia, Turkey, Ukraine, Ukraine, United Arab Emirates, Uzbekistan, Venezuela and Viet Nam.	

APPENDIX 6 LIST OF NOVO NORDISK ENTITIES SUBJECT TO BCRs

[Please refer to separately attached document]