

# Novo Nordisk Binding Corporate Rules

## PART I: BACKGROUND AND ACTIONS

### WHAT IS DATA PROTECTION LAW?

Data protection law gives people the right to control how their “personal information”<sup>1</sup> is used. When Novo Nordisk collects and uses the personal information of its employees, contractors, business contacts and other third parties this is covered and regulated by data protection law.

### HOW DOES DATA PROTECTION LAW AFFECT NOVO NORDISK INTERNATIONALLY?

Data protection law does not allow the transfer of personal information to countries outside Europe<sup>2</sup> that do not ensure an adequate level of data protection. Some of the countries in which Novo Nordisk operates are not regarded by European data protection authorities as providing an adequate level of protection for individuals’ data privacy rights.

### WHAT IS NOVO NORDISK DOING ABOUT IT?

To avoid breaking the law Novo Nordisk must take proper steps to ensure that its use of personal information on an international basis is safe and, hence, lawful. The purpose of this Policy, therefore, is to set out a framework to satisfy the standards contained in European data protection law and, as a result, provide an adequate level of protection for all personal information used and collected in Europe and transferred from the Novo Nordisk entities within Europe to Novo Nordisk entities outside Europe.

Although the legal obligations under European law apply only to personal information used and collected in Europe, Novo Nordisk will apply this Policy globally, and in **all cases** where Novo Nordisk processes personal information both manually and by automatic means and whether the personal information relates to Novo Nordisk’s employees, contractors, business contacts or other third parties.<sup>3</sup>

Central to this Policy are 15 Rules based on, and interpreted in accordance with, relevant European data protection standards that must be followed by each employee or contractor when handling personal information. All Novo Nordisk entities are legally bound to comply with this Policy.

---

<sup>1</sup> Personal information means any information relating to an identified or identifiable natural person in line with the definition of “personal data” in Directive 95/46/EC.

<sup>2</sup> For the purpose of this Policy reference to Europe means the EEA **and** Switzerland

<sup>3</sup> Processing in European data protection law means any set of operations performed upon personal information whether or not by automatic means. This is interpreted widely to include collecting, storing, organising, destroying, amending, consulting, destroying and disclosure of the personal information.

## **WHAT DOES THIS MEAN IN PRACTICE FOR PERSONAL INFORMATION COLLECTED AND USED IN THE EEA?**

European data protection law states that Novo Nordisk's employees, contractors, business contacts and other third parties whose personal information is used and/or collected in Europe and transferred to Novo Nordisk entities outside Europe must be able to benefit from certain rights to enforce the Rules set out in this Policy and these individuals will have the right to:

- seek enforcement of compliance with this Policy, including its appendices;
- lodge a complaint with a European data protection authority of competent jurisdiction and/or to take action against the Novo Nordisk entity established in Europe and responsible for exporting the personal information in the courts of the jurisdiction in which that Novo Nordisk entity established in order to enforce compliance with this Policy, including its appendices;
- make complaints to a Novo Nordisk entity established in Europe in accordance with the Data Protection Binding Corporate Rules Complaint Handling Procedure, seek appropriate redress from the Novo Nordisk entity established in Europe and responsible for exporting the information, including the remedy of any breach of the Policy by any Novo Nordisk entity outside Europe and, where appropriate, receive compensation from the Novo Nordisk entity established in Europe and responsible for exporting the personal information for any damage suffered as a result of a breach of this Policy by Novo Nordisk in accordance with the determination of a court or other competent authority;
- obtain a copy of this Policy (which will be available online from [www.novonordisk.com](http://www.novonordisk.com)) and the unilateral declaration made by Novo Nordisk A/S in connection with this Policy.

In the event of a claim being made in which an individual has suffered damage where that individual can demonstrate that it is likely that the damage has occurred because of a breach of the Policy, Novo Nordisk has agreed 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 Novo Nordisk entity responsible for exporting the personal information to that entity outside Europe.

Novo Nordisk A/S has a system in place to oversee and ensure compliance with all aspects of this Policy. The governance of the Policy is the responsibility of a corporate compliance support function reporting to the General Counsel. The corporate compliance support function is supported by local lawyers at regional and country level who are responsible for overseeing and ensuring compliance with this Policy on a day-to-day basis.

### **FURTHER INFORMATION**

If you have any questions regarding the provisions of this Policy, your rights under this Policy or any other data protection issues you may contact Novo Nordisk's corporate compliance support function that will either deal with the matter or forward it to the appropriate person or department within Novo Nordisk at the following address:

**Data Protection Officer**  
[privacy@novonordisk.com](mailto:privacy@novonordisk.com)  
**+45 44448888**

**Novo Nordisk A/S**  
**Novo Alle,**  
**DK-2880 Bagsværd**  
**Denmark**

The corporate compliance support function is responsible for ensuring that changes to this Policy are notified to the Novo Nordisk entities and to individuals whose personal information is processed by Novo Nordisk.

## **PART II: THE RULES**

The Rules are divided into two sections. Section A addresses the basic principles of European data protection law Novo Nordisk must observe when Novo Nordisk collects and uses personal information.

Section B deals with the practical commitments made by Novo Nordisk to the European data protection authorities in connection with this Policy.

### **Section A**

#### **RULE 1 – COMPLIANCE WITH LOCAL LAW**

**Rule 1 – Novo Nordisk will first and foremost comply with local law where it exists.**

As an organisation, Novo Nordisk will always comply with any applicable legislation relating to personal data (e.g. in Denmark, the Danish Act on Processing of Personal Data No.429 of 31 May 2000) and will ensure that where personal information is collected and used this is done in accordance with the local law.

Where there is no law or the law does not meet the standards set out by the Rules in this Policy, Novo Nordisk's position will be to process personal information adhering to the Rules in this Policy.

#### **RULE 2 – ENSURING TRANSPARENCY AND USING PERSONAL INFORMATION FOR A KNOWN PURPOSE ONLY**

**Rule 2A – Novo Nordisk will explain to individuals, at the time their personal information is collected, how that information will be used.**

Novo Nordisk will ensure that individuals are always told in a clear and comprehensive way (usually by means of a fair processing statement) about the uses and disclosures made of their information (including the secondary uses and disclosures of the information) when such information is obtained or, if not practicable to do so at the point of collection, as soon as possible after that, unless there is a legitimate basis for not doing so, for example; where it is necessary to safeguard national security or defence, for the prevention or detection of crime, taxation purposes, legal proceedings or where otherwise permitted by law.

**Rule 2B – Novo Nordisk will only obtain and use personal information for those purposes which are known to the individual or which are within their expectations and are relevant to Novo Nordisk.**

This rule means that Novo Nordisk will identify and make known the purposes for which personal information will be used (including the secondary uses and

disclosures of the information) when such information is obtained or, if not practicable to do so at the point of collection, as soon as possible after that, unless there is a legitimate basis for not doing so as described in Rule 2A.

**Rule 2C – Novo Nordisk will only change the purpose for which personal information is used if Novo Nordisk make people aware of such change or it is within their expectations and they can express their concerns.**

If Novo Nordisk collects personal information for a specific purpose (as communicated to the individual via the relevant fair processing statement) and subsequently Novo Nordisk wishes to use the information for a different or new purpose, the relevant individuals will be made aware of such a change unless there is a legitimate basis for not doing so as described in Rule 2A above. In certain cases, the individual's consent to the new uses or disclosures will be necessary.

### **RULE 3 – ENSURING DATA QUALITY**

**Rule 3A – Novo Nordisk will keep personal information accurate and up to date.**

The main way of ensuring that personal information is kept accurate and up to date is by actively encouraging individuals to inform Novo Nordisk when their personal information changes.

**Rule 3B – Novo Nordisk will only keep personal information for as long as is necessary.**

Novo Nordisk will comply with the Novo Nordisk Procedure for Document and Record Retention Management (as amended from time to time) which sets out a set of general requirements for documents and records applicable globally throughout Novo Nordisk.

**Rule 3C – Novo Nordisk will only keep personal information which is adequate relevant and not excessive.**

Novo Nordisk will identify the minimum amount of personal information that is required in order properly to fulfil its purpose.

### **RULE 4 – TAKING APPROPRIATE SECURITY MEASURES**

**Rule 4A – Novo Nordisk will always adhere to its IT Security Policies.**

Novo Nordisk will comply with the requirements in the Computer Systems Standardisation and Security Procedure as revised and updated from time to time together with any other security procedures relevant to a business area or function.

**Rule 4B – Novo Nordisk will ensure that providers of services to Novo Nordisk also adopt appropriate and equivalent security measures.**

European law expressly requires that where a provider of a service to any of the Novo Nordisk entities has access to customers', contractors, business contacts or employees' personal information (e.g. a payroll provider), strict contractual obligations dealing with the security of that information are imposed to ensure that such service providers act only on Novo Nordisk's instructions when using that information and that they have in place proportionate technical and organisational security measures to safeguard the personal information.

**Rule 4C- Where Novo Nordisk entities process personal information on behalf of other Novo Nordisk entities those entities will adhere to Rule 4A and act only on the instructions of the Novo Nordisk entity on whose behalf the processing is carried out.**

Where a service provider is a Novo Nordisk entity processing personal information on behalf of another Novo Nordisk entity the Novo Nordisk service provider must act only on the written instructions of the Novo Nordisk entity on whose behalf the processing is carried out and ensure that it has in place proportionate technical and organisational security measures to safeguard the personal information.

## **RULE 5 – HONOURING INDIVIDUALS' RIGHTS**

**Rule 5A – Novo Nordisk will adhere to the Subject Access Procedure and will be receptive to any queries or requests made by individuals in connection with their personal information.**

Individuals are entitled (by making a written request to Novo Nordisk) to be supplied with a copy of any personal information held about them (including both electronic and paper records). Novo Nordisk will follow the steps set out in the Subject Access Procedure (see Appendix 1) when dealing with subject access requests.

**Rule 5B – Novo Nordisk will deal with requests to delete, rectify or block inaccurate personal information or to cease processing personal information in accordance with the Subject Access Procedure.**

Individuals are entitled to rectification, deletion or blocking, as appropriate, of personal information which is shown to be inaccurate and, in certain circumstances, to object to the processing of their personal information. Novo Nordisk will follow the steps set out in the Subject Access Procedure (see Appendix 1) in such circumstances.

## **RULE 6 – ENSURING ADEQUATE PROTECTION FOR OVERSEAS TRANSFERS**

**Rule 6 – Novo Nordisk will not transfer personal information to third parties outside Novo Nordisk without ensuring adequate protection for the information in accordance with the standards set out by this Policy.**

In principle, international transfers of personal information to third parties outside the Novo Nordisk entities are not allowed without appropriate steps being taken; for example, contractual clauses (such as the EU standard contractual clauses) which will protect the personal information being transferred.

## **RULE 7 – SAFEGUARDING THE USE OF SENSITIVE PERSONAL INFORMATION**

**Rule 7A – Novo Nordisk will only use sensitive personal information if it is absolutely necessary to use it.**

Sensitive personal information is information relating to an individual's racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life and criminal convictions. Novo Nordisk will assess whether sensitive personal information is required for the proposed use and when it is absolutely necessary in the context of the business.

**Rule 7B – Novo Nordisk will only use sensitive personal information where the individual's express consent has been obtained unless Novo Nordisk has a legitimate basis for doing so**

In principle, individuals must expressly agree to the collection and use of sensitive personal information by Novo Nordisk unless Novo Nordisk has a legitimate basis for doing so. This permission to use sensitive personal information by Novo Nordisk must be genuine and freely given.

## **RULES – LEGITIMISING DIRECT MARKETING**

**Rule 8A – Novo Nordisk will allow customers to opt out of receiving marketing information.**

One of the data protection rights that individuals have is the right to object to the use of their personal information for direct marketing purposes and Novo Nordisk will honour all such opt out requests.

**Rule 8B – Novo Nordisk will suppress from marketing initiatives the personal information of individuals who have opted out of receiving marketing information.**

Novo Nordisk will take all necessary steps to prevent the sending of marketing materials to individuals who have opted out.

## **RULE 9 – AUTOMATED INDIVIDUAL DECISIONS**

**Rule 9 - Where decisions are made by automated means, individuals will have the right to know the logic involved in the decision and Novo Nordisk will take necessary measures to protect the legitimate interests of individuals.**

There are particular requirements in place under European data protection law to ensure that no evaluation of, or decision about, a data subject which significantly affects them can be based solely on the automated processing of personal information unless measures are taken to protect the legitimate interests of individuals.

## **SECTION B**

### **RULE 10 – TRAINING**

**Rule 10 – Novo Nordisk will provide appropriate training to employees who have permanent or regular access to personal information, who are involved in the collection of personal information or in the development of tools used to process personal information.**

### **RULE 11 – AUDIT**

**Rule 11 – Novo Nordisk will comply with the Data Protection Binding Corporate Rules Policy Audit Protocol set out in Appendix 2.**

### **RULE 12 – COMPLAINT HANDLING**

**Rule 12 - Novo Nordisk will comply with the Data Protection Binding Corporate Rules Policy Complaint Handling Procedure set out in Appendix 3**

### **RULE 13 – COOPERATION WITH DATA PROTECTION AUTHORITIES**

**Rule 13 – Novo Nordisk will comply with the Data Protection Binding Corporate Rules Policy Co-operation Procedure set out in Appendix 4.**

### **RULE 14 – UPDATE OF THE RULES**

**Rule 14 – Novo Nordisk will comply with the Data Protection Binding Corporate Rules Policy Updating Procedure set out in Appendix 5.**

**RULE 15 – ACTIONS IN CASE OF NATIONAL LEGISLATION PREVENTING RESPECT FOR THE POLICY**

**Rule 15A – Novo Nordisk will ensure that where it has reason to believe that the legislation applicable to it prevents it from fulfilling its obligations under the Policy and which has a substantial effect on its ability to comply with the Policy, Novo Nordisk will promptly inform the chief compliance officer unless otherwise prohibited by a law enforcement authority.**

**Rule 15B – Novo Nordisk will ensure that where there is a conflict between the national law and this Policy the chief compliance officer will make a responsible decision on the action to take and will consult the data protection authority with competent jurisdiction in case of doubt.**



## **PART III – APPENDICES**

### **APPENDIX 1 SUBJECT ACCESS PROCEDURE**

#### **1. SUBJECT ACCESS PROCEDURE**

- 1.1 European Data Protection law gives individuals whose personal information is collected and/or used in Europe<sup>4</sup> the right to be informed whether any personal information about them is being processed by an organisation. This is known as the right of subject access.
- 1.2 Individuals whose personal information is collected and/or used in Europe and/or transferred between Novo Nordisk entities under the Novo Nordisk Data Protection Binding Corporate Rules Policy will also benefit from the right of subject access. This Subject Access Procedure explains how Novo Nordisk deals with a subject access request relating to such personal information (referred to as “valid request” in this Procedure).
- 1.3 Where a subject access request is subject to European data protection law because it is made in respect of personal information collected and/or used in Europe, such a request will be dealt with by Novo Nordisk in accordance with this Procedure, but where the applicable European data protection law differs from this Procedure, the local data protection law will prevail.
- 1.4 An individual making a valid request to Novo Nordisk is entitled to:
  - 1.4.1 Be informed whether Novo Nordisk holds and is processing personal information about that person.
  - 1.4.2 Be given a description of the personal information, the purposes for which they are being held and processed and the recipients or classes of recipient to whom the information is, or may be, disclosed by Novo Nordisk.
  - 1.4.3 Communication in intelligible form of the personal information held by Novo Nordisk

---

<sup>4</sup> In this policy Europe means the EEA plus Switzerland

- 1.5 The request must be made in writing, which can include email<sup>5</sup>.
- 1.6 Under normal circumstances no fee will be applied
- 1.7 Novo Nordisk must respond to a valid request within [20] working days of receipt of that request.
- 1.8 Novo Nordisk may ask for such information which it may reasonably require in order to confirm the identity of the individual making the request and to locate the information which that person seeks.

## **2. PROCEDURE**

### 2.1 Receipt of a Subject Access Request

2.1.1 If any employee or subcontractor of Novo Nordisk receives any request from an individual for their personal information, they must pass the communication to the local legal and compliance unit immediately upon receipt indicating the date on which it was received together with any other information which may assist the local legal and compliance officer to deal with the request.

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

### 2.2 Initial Steps

2.2.1 The local legal and compliance officer will make an initial assessment of the request to decide whether it is a valid request and whether confirmation of identity, or any further information, is required.

2.2.2 The local legal and compliance officer will then contact the individual in writing to confirm receipt of the subject access 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 subject access

2.3.1 A valid request may be refused on the following grounds;

---

<sup>5</sup> Unless the local data protection law provides that an oral request may be made, in which case Novo Nordisk will record the request and provide a copy to the individual making the request before dealing with it.

- (a) Where the subject access request is made to a European Novo Nordisk entity and relates to the use or collection of personal information by that entity, if the refusal to provide the information is consistent with the data protection law within that jurisdiction, or;
- (b) Where the subject access request does not fall within 2.3.1(a) and;
  - (i) if, in the opinion of Novo Nordisk it is necessary to do so to safeguard the legitimate business interests of Novo Nordisk, national or public security, defence, the prevention, investigation, detection and prosecution of criminal offences, for the protection of the data subject or of the rights and freedoms of others; or
  - (ii) if the personal information held by Novo Nordisk is processed by or on behalf of Novo Nordisk solely for scientific purposes or are kept as personal information for a period which does not exceed the period necessary for the sole purpose of creating statistics; or
  - (iii) if the personal information is held by Novo Nordisk in non-automated form and is not or will not become part of a filing system.

## 2.4 The Search and the Response

- 2.4.1 The local privacy compliance officer will arrange a search of all relevant electronic and paper filing systems.
- 2.4.2 The local legal and compliance officer may refer any complex cases to the Chief Compliance officer for advice, particularly where the request includes information relating to third parties or where the release of personal information may prejudice commercial confidentiality or legal proceedings.
- 2.4.3 The information requested will be collated by the local legal and compliance officer into a readily understandable format (internal codes or identification numbers used at Novo Nordisk that correspond to personal data shall be translated before being disclosed). A covering letter will be prepared by the local legal and compliance officer which includes information required to be provided in response to a subject access request.

- 2.4.4 Where the provision of the information in permanent form is not possible or would involve disproportionate effort there is no obligation to provide a copy of the information. The other information referred to in 1.2 above must still be provided. In such circumstances the individual may be offered the opportunity to have access to the information by inspection or to receive the information in another form.
- 2.5 Requests for deletion, rectification or blocking of personal information
- 2.5.1 If a request is received for the deletion, rectification or blocking of that individual's personal information, such a request must be considered and dealt with as appropriate by the local legal and compliance officer.
- 2.5.2 If a request is received advising of a change in that individual's personal information, such information must be rectified or updated accordingly if Novo Nordisk is satisfied that there is a legitimate basis for doing so
- 2.5.3 If the request is to cease processing that individuals' personal information because the rights and freedoms of the individual are prejudiced by virtue of such processing by Novo Nordisk, or on the basis of other compelling legitimate grounds, the matter will be referred by the local legal and compliance officer to the Chief Compliance Officer to assess. Where the processing undertaken by Novo Nordisk is required by law, the request will not be regarded as valid.
- 2.6 All queries relating to this policy are to be addressed to the local legal and compliance officer.

## **APPENDIX 2**

### **DATA PROTECTION BINDING CORPORATE RULES POLICY AUDIT PROTOCOL**

#### **1. Background**

The purpose of the Data Protection Binding Corporate Rules Policy ("Policy") is to safeguard personal information transferred between the Novo Nordisk entities. The Policy requires approval from the data protection authorities in the European member states from which the personal information is transferred. One of the requirements of the data protection authorities is that Novo Nordisk audits compliance with the Policy and satisfies certain conditions in so doing and this document describes how Novo Nordisk deals with such requirements.

#### **2. Approach**

##### 2.1 Scope of audit

Novo Nordisk's Audit Functions will be responsible for performing the audits (although from time to time Novo Nordisk may appoint third party auditors to carry out the audits on its behalf in accordance with clause 2.4 below) and will ensure that such audits address all aspects of the Policy, including all IT systems, databases, security policies, training, privacy policies and contractual provisions in place within Novo Nordisk in respect of the Policy.

##### 2.2 Responsibility for compliance

Novo Nordisk's Audit Functions will be responsible for ensuring that any issues or instances of non-compliance are brought to the attention of Novo Nordisk's Executive Management which is committed to ensuring that any corrective actions take place as soon as is reasonably possible.

##### 2.3 Timing

Audit of the Policy will take place annually or within a shorter timescale at the instigation of Novo Nordisk's Audit Functions. The scope of the audit performed annually will be decided by Novo Nordisk's Audit Functions based on a risk and materiality assessment which will be updated annually.

## 2.4 Auditors

Audit of the Policy will be undertaken by Novo Nordisk's Audit Functions but reliance on work performed by other accredited internal/external auditors may be determined by Novo Nordisk's Audit Functions. Novo Nordisk's Audit Functions will manage and provide quality assurance of audit work performed by others.

## 2.5 Report

Novo Nordisk has agreed to provide copies of the results of any audit of the Policy to a European data protection authority of competent jurisdiction upon request subject to applicable law and respect for the confidentiality and trade secrets of the information provided. Novo Nordisk's Audit Functions will be responsible for liaising with the European data protection authorities for this purpose. In addition, Novo Nordisk has agreed that in data protection authorities may audit the Novo Nordisk entities for the purpose of reviewing compliance with the Policy in accordance with the provisions of clause 5 of the Co-operation Procedure<sup>6</sup>. Novo Nordisk's Audit Functions will also be responsible for liaising with the European data protection authorities for this purpose.

---

<sup>6</sup> Clause 5 states that "Where any Novo Nordisk entity is located within the jurisdiction of a data protection authority based in Europe, Novo Nordisk agrees that that data protection authority may audit that Novo Nordisk entity for the purpose of reviewing compliance with the Policy, 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 information is transferred under the Policy, on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of Novo Nordisk".

## **APPENDIX 3**

### **DATA PROTECTION BINDING CORPORATE RULES POLICY COMPLAINT HANDLING PROCEDURE**

#### **Data Protection Binding Corporate Rules Policy Complaint Handling Procedure**

##### **Background**

The Data Protection Binding Corporate Rules Policy ("**Policy**") safeguards personal information transferred between the Novo Nordisk entities. The content of the Policy is determined by the data protection authorities in the European member states from which the personal information is transferred and one of their requirements is that Novo Nordisk must have a complaint handling procedure in place. The purpose of this procedure is to explain how complaints brought by an individual whose personal information is processed by Novo Nordisk under the Policy are dealt with.

##### **How individuals can bring complaints:**

Individuals can bring complaints in writing by contacting their local Novo Nordisk legal and compliance unit. Complaints may also be addressed to the Data Protection Officer via [privacy@novonordisk.com](mailto:privacy@novonordisk.com).

##### **Who handles complaints?**

The local Novo Nordisk legal and compliance unit will handle all complaints arising under the Policy. The local Novo Nordisk legal and compliance unit will liaise with colleagues from relevant business and support units as appropriate to deal with complaints.

##### **What is the response time?**

Unless exceptional circumstances apply, the Data Protection Officer will acknowledge receipt of a complaint to the individual concerned within 5 working days, investigating and making a substantive response within one month. If, due to the complexity of the complaint, a substantive response cannot be given within this period, the Data Protection Officer will advise the complainant accordingly and provide a reasonable estimate (not exceeding six months) for the timescale within which a response will be provided.

##### **Disputing a finding**

Certain individuals whose personal information is collected and/or used and in accordance with European data protection law have rights under the Policy to complain to a European data protection authority and/or to 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.



## **APPENDIX 4**

### **DATA PROTECTION BINDING CORPORATE RULES POLICY CO-OPERATION PROCEDURE**

#### **Data Protection Binding Corporate Rules Policy Co-operation Procedure**

1. This Data Protection Binding Corporate Rules Policy Co-operation Procedure sets out the way in which Novo Nordisk will co-operate with the European<sup>7</sup> data protection authorities in relation to the Novo Nordisk Data Protection Binding Corporate Rules Policy ("Policy").
2. Where required, Novo Nordisk will make the necessary personnel available for dialogue with a European data protection authority in relation to the Policy.
3. Novo Nordisk will actively review and consider:
  - any decisions made by relevant European data protection authorities on any data protection law issues that may affect the Policy; and
  - the views of the Article 29 Working Party as outlined in its published guidance on Binding Corporate Rules.
4. Novo Nordisk will provide upon request copies of the results of any audit of the Policy to a European data protection authority of competent jurisdiction subject to applicable law and respect for the confidentiality and trade secrets of the information provided.
5. Where any Novo Nordisk entity is located within the jurisdiction of a data protection authority based in Europe, Novo Nordisk agrees that that data protection authority may audit that Novo Nordisk entity for the purpose of reviewing compliance with the Policy, 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 information is transferred under the Policy, on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of Novo Nordisk.

---

<sup>7</sup> References to Europe for the purposes of this document includes the EEA and Switzerland

6. Novo Nordisk agrees to abide by a formal decision of the applicable data protection authority which is final and against which no further appeal is possible on any issues related to the interpretation and application of the Policy.

## APPENDIX 5

### DATA PROTECTION BINDING CORPORATE RULES POLICY UPDATING PROCEDURE

#### Data Protection Binding Corporate Rules Policy Updating Procedure

- 1. This Data Protection Authority Updating Procedure sets out the way in which Novo Nordisk will communicate changes to the Novo Nordisk Data Protection Binding Corporate Rules Policy ("Policy") to the European<sup>8</sup> data protection authorities, data subjects and to the Novo Nordisk entities bound by the Policy.**
2. Novo Nordisk will communicate any material changes to the Policy to the Datatilsynet and any other relevant European data protection authorities at least once a year. However, Novo Nordisk does not expect to have to communicate changes to the BCR which are administrative in nature or which have occurred as a result of a change of applicable data protection law in any European country, through any legislative, court or supervisory authority measure unless they result in a substantive change to the BCR. Novo Nordisk will also provide a brief explanation of the reasons for any notified changes to the Policy.
3. Novo Nordisk will communicate any changes to the Policy to the Novo Nordisk entities bound by the Policy and to the data subjects who benefit from the Policy. The Policy contains a change log which sets out the date the Policy is revised and the details of any revisions made.
4. By way of delegated authority from the General Counsel, the appointed officer will maintain an up to date list of the Novo Nordisk entities and ensure that all new Novo Nordisk entities are bound by the Policy before a transfer of personal information to them takes place. Novo Nordisk will communicate any substantial changes to the list of Novo Nordisk entities once a year. Otherwise, Novo Nordisk will communicate an up to date list of entities to the Datatilsynet and any other relevant European data protection authorities when required.

---

<sup>8</sup> References to Europe for the purposes of this document includes the EEA and Switzerland

## **Schedule 1 – Third Party Beneficiary Rights**

In accordance with Clause 7, individuals whose Personal Information is processed by a Novo Nordisk Entity and is subject to the BCR shall be able to enforce the following third party beneficiary rights against the appropriate Exporting Entity (as defined in Clause 7) :

- To seek enforcement of compliance with the BCR, including its appendices;
- To lodge a complaint with a European data protection authority of competent jurisdiction and/or to take action against a Novo Nordisk Entity as set out in Clause 7 in the courts of the jurisdiction in which the Exporting Entity responsible for exporting the personal information is established in order to enforce compliance with the BCR.
- To make complaints to a Novo Nordisk Entity within Europe in accordance with the Data Protection Binding Corporate Rules Complaint Handling Procedure, seek appropriate redress from an Exporting Entity as described in Clause 7, including the remedy of any breach of the BCR by any Importing Entity and, where appropriate, receive compensation from an Exporting Entity for any damage suffered as a result of a breach of the BCR in accordance with the determination of a court or other competent authority.
- To obtain a copy of the BCR and this unilateral declaration on request.