Novo Nordisk Binding Corporate Rules

INTRODUCTION TO THE DATA PROTECTION BINDING CORPORATE RULES POLICY

This Data Protection Binding Corporate Rules Policy ("**Policy**"), which forms part of the Novo Nordisk Way of Management, establishes Novo Nordisk's approach to compliance with European data protection law and specifically to transfers of personal information between the Novo Nordisk entities.

This Policy applies to all Novo Nordisk entities and their employees and contains 15 rules ("**Rules**"). Novo Nordisk must comply with and respect this Policy when collecting and using personal information. This Policy does not replace any specific data protection requirements that might apply to a business area or function.

This Policy applies to all personal information of employees, customers, suppliers and other third parties, wherever it is collected and used as part of the regular business activities of Novo Nordisk. Transfers of personal information take place between the Novo Nordisk entities during the normal course of business and such information may be stored in centralised databases accessible by Novo Nordisk entities from anywhere in the world.

This Policy will also apply where Novo Nordisk entities process personal information on behalf of other Novo Nordisk entities.

This Policy will be published on the website accessible at www.novonordisk.com

PART I: BACKGROUND AND ACTIONS

WHAT IS DATA PROTECTION LAW?

Data protection law gives people the right to control how their "personal information"[1] 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[2] 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.[3]

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.

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

---

[1] 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.

[2] For the purpose of this Policy reference to Europe means the EEA **and** Switzerland

[3] 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.

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) 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
+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.

RULE8 – 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.